AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

VOLUME LXI

1939

THE JOHNS HOPKINS PRESS
BALTIMORE, MARYLAND
U. S. A.

AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

PUBLISHED UNDER THE JOINT AUSPICES OF

THE JOHNS HOPKINS UNIVERSITY
AND
THE AMERICAN MATHEMATICAL SOCIETY

Volume LXI, Number 1
JANUARY, 1939

THE JOHNS HOPKINS PRESS
BALTIMORE, MARYLAND
U. S. A.

CONTENTS

The American Journal of Mathematics will appear four times yearly.

The subscription price of the Journal for the current volume is $7.50 (foreign postage 50 cents); single numbers $2.00.

A few complete sets of the Journal remain on sale.

Papers intended for publication in the Journal may be sent to any of the Editors.

Editorial communications may be sent to Dr. A. Cohen at The Johns Hopkins University.

Subscriptions to the Journal and all business communications should be sent to The Johns Hopkins Press, Baltimore, Maryland, U. S. A.

Entered as second-class matter at the Baltimore, Maryland, Postoffice, acceptance for mailing at special rate of postage provided for in Section 1103, Act of October 3, 1917, Authorized on July 3, 1918.

PRINTED IN THE UNITED STATES OF AMERICA
BY J. H. FURST COMPANY, BALTIMORE, MARYLAND

THE SIGNIFICANCE OF THE SYSTEM OF SUBGROUPS FOR THE STRUCTURE OF THE GROUP.*

By Reinhold Baer.

DEDICATED TO

FELIX HAUSDORFF

On his 70th Birthday, November 8, 1938.

Theorems in group theory whose proofs are effected by manipulating subgroups and not elements—such theorems generally refer to direct decompositions—are as a rule easily recognized as special cases of theorems in the theory of lattices. There are other theorems in the theory of groups where such a generalization is not quite obvious. Thus the problem arises to characterize those parts of the theory of groups in which the results may be expected to be special cases of theorems in the theory of lattices. Such a part of the theory of groups contains but one essentially group-theoretical statement, namely the assertion that all the facts in this theory are special cases of results in the theory of lattices.

If the group G is isomorphic to every group with an isomorphic lattice of subgroups, then it may be said that the structure theory of this group G forms part of the theory of lattices. If in addition every isomorphism of the lattice of the subgroups of G is induced by an isomorphism of G, then the relative structure of the subgroups of G presents a problem which belongs to the theory of lattices.

Thus it will be our problem to discuss the relations between the isomorphisms of groups on the one hand and the isomorphisms of the lattice of its subgroups on the other hand. The term "isomorphism of the lattice of subgroups" will be used in a more or less restricted sense. In its broadest meaning this term refers only to lattice properties in the accepted sense of the word, whereas the isomorphisms of the lattice of the subgroups in the more restricted sense of the term shall preserve properties like normality and numbers like the index.

The modern development of the theory of lattices has been preceded by a discussion of the above problem. It has been proved in 1928 by A. Rottlaender that there exists finite non-isomorphic groups whose lattices of subgroups are isomorphic in a rather strong sense.[1] Since these groups are both not abelian,

---

* Presented to the American Mathematical Society, Sept. 6, 1938.

[1] Ada Rottlaender, "Nachweis der Existenz nicht-isomorpher Gruppen von gleicher Situation der Untergruppen," *Mathematische Zeitschrift*, Bd. 28 (1928), pp. 641-653.

one might feel inclined to discard this example, considering that lattice theory is primarily concerned with abelian questions. But Rottlaender proved at the same time that there exist two groups of order p^3 with isomorphic lattices of subgroups one of which is abelian and the other not.[2] Furthermore one should bear in mind that any two groups of prime number order have isomorphic lattices of subgroups and that there exist abelian groups of prime power order, possessing automorphisms of the lattice of subgroups which are not induced by automorphisms of the group.[3]

It is the object of this investigation to show that these phenomena are—at least as far as abelian groups are concerned—rather the exception than the rule. In a somewhat crude form one might state as our main result that every isomorphism of the lattice of subgroups of an abelian group which is not "too small" is induced by an isomorphism of the group in question.

A precise sattement of our concepts and principal results may be found in section **1**. As the difficulties in our investigation arise mostly from the "smaller" groups, these will be treated to some extent before we embark on the proofs of our main theorems.

1. A function f of the subgroups of the group G is called a *subgroup-isomorphism of G upon the group G'*, if

(1. a) S^f is a subgroup of G' for every subgroup S of G;

(1. b) to every subgroup S' of G' there exists a subgroup S of G such that $S^f = S'$;

(1. c) $S \leq T$ is a necessary and sufficient condition for $S^f \leq T^f$.

Thus a subgroup-isomorphism of G upon G' defines a one-one-correspondence between the subgroups of G and the subgroups of G' and the inverse function to a subgroup-isomorphism is a subgroup-isomorphism. Moreover a subgroup-isomorphism maps the meet and join of a certain set of subgroups upon the meet and join of the corresponding subgroups and in particular the group-unit upon the group-unit and G upon G'. A subgroup-isomorphism of G upon G' is therefore an isomorphism of the lattice of all the subgroups of G upon the lattice of all the subgroups of G'.—If in particular $G = G'$, then the subgroup-isomorphisms of G upon G' are called *subgroup-automorphisms of G*.

If S is a subgroup of T, then the index $[T:S]$ is the number of different classes of T mod S. A subgroup-isomorphism f of G upon G' is called *index-preserving*, if

[2] Rottlaender, *op. cit.*, pp. 644-647.

[3] Reinhold Baer, "Situation der Untergruppen und Struktur der Gruppe, *Sitz.-Ber. Heidelberger Akad. Wiss.; Math.-nat. Kl.* 1933 (2), pp. 12-17.

(1. d) $[T:S] = [T^f : S^f]$ for subgroups S of *cyclic* subgroups T of G; and f is called *strictly index-preserving,* if

(1. d*) $[T:S] = [T^f : S^f]$ for subgroups S of subgroups T of G.

The subgroup-isomorphism f of the group G upon the group G' is *normal,* if it satisfies:

(1. e) S is a *normal* subgroup of G if, and only if, S^f is a *normal* subgroup of G';

and f is said to be *strictly normal,* if it satisfies:

(1. e*) The subgroups R and S of the subgroup T of G are conjugate in T if, and only if, R^f and S^f are conjugate subgroups of T^f.

Since strictly index-preserving subgroup-isomorphisms preserve the orders of the subgroups, the strictly index-preserving and strictly normal subgroup-isomorphisms are exactly the same as the correspondences which preserve the situation of the subgroups [Rottlaender]. The result of Rottlaender, mentioned in the introduction, may now be stated in the form:

there exist finite groups which are not isomorphic, though there exists a strictly index-preserving and strictly normal subgroup-isomorphism between them.

If there is any danger of confusion, then the isomorphisms between groups in the customary sense of the word will be termed *element-isomorphisms.* It is obvious that every element-isomorphism of the group G upon the group G' induces a uniquely determined strictly index-preserving and strictly normal subgroup-isomorphism of G upon G'. But as has been remarked before, there exist strictly index-preserving subgroup-automorphisms of finite abelian groups (which are of course strictly normal) which are not induced by element-automorphisms.

The following theorem which will not be used in the future may serve as an illustration of these concepts.

If G is either an alternating or a symmetric group of finite degree n, and if f is a strictly index-preserving and normal subgroup-isomorphism of G upon the group G', then G and G' are (element-)isomorphic.

Proof. It is a well known fact that the symmetric group of degree n is apart from isomorphic groups the only group of order $n!$ which contains a subgroup of index n such that no subgroup $\neq 1$ of this subgroup is normal in

the whole group and the same property together with the fact that the order is $n!/2$ characterizes the alternating group. Now the theorem is obvious.

The principal results of this investigation may be stated in the following form:

The subgroup-isomorphism f of the group G is induced by an element-isomorphism of G, if one of the following conditions is satisfied:

(1) G is hamiltonian [4] and all the elements in G are of even order.

(2) G is abelian and contains at least two independent elements of infinite order.

(3) G is abelian, does not contain elements of infinite order, contains elements of order p^2, if it contains elements of the prime number order p, and G contains at least three independent elements of order n, if it contains elements of order n.

(4) G is abelian, all its elements $\neq 1$ have the same finite order p, G contains at least p^3 elements and all the elements $\neq 1$ in G^f have the same order.

The subgroup-isomorphism f maps the group G upon an isomorphic group H, if one of the following conditions is satisfied:

(5) G is abelian and contains elements of infinite order, f is index-preserving, and H is abelian.

(6) G is abelian, does not contain elements of infinite order, the number of elements of order p in G is $\neq p$, and H is abelian.

(7) G is abelian, does not contain elements of infinite order, and f is index-preserving as well as normal.

The following discussion is devoted to the proofs of these statements. It will be seen from suitable examples that it is impossible to omit any part of any of the above conditions. No attempt has been made to give a systematic survey of the possible counter examples—in particular a theory of the groups which are subgroup-isomorphic with abelian groups—though some indications are contained in this investigation.

2. Finite cyclic groups.

(2.1) *The group G is a cyclic group whose order is the n-th power of a prime number if, and only if,*

[4] A group is hamiltonian, if it is not abelian, but all its subgroups are normal.

(a) *the number of subgroups of G is $n+1$;*

(b) *$S \leq T$ or $T \leq S$ for any two subgroups S and T of G.*

Proof. If G is a cyclic group of prime power order p^n, then its subgroups are just the subgroups G^{p^i} for $0 \leq i \leq n$ and this proves the necessity of the conditions.—If the group G satisfies the conditions (a) and (b), then G contains a subgroup $W \neq G$ which contains every subgroup $\neq G$. Any element w of G which is not an element of W generates G and G is consequently a cyclic group. If m is the order of the cyclic group G — G is clearly a finite group — and if p is a prime number, dividing m, then $G^p = W$ and this shows that $m = p^n$.

An obvious corollary of (2.1) is

(2.2) *Suppose that G is a cyclic group of prime power order p^n. Then G and the group H are subgroup-isomorphic if, and only if, H is a cyclic group of prime power order q^n.*

If $n_1, \cdots, n_k$ are not-negative integers, then the *lattice* $L(n_1, \cdots, n_k)$ consists of the k-tuples $(m_1, \cdots, m_k)$ which satisfy $0 \leq m_i \leq n_i$ for every i and the partial order in L is defined by

$$(m_1, \cdots, m_k) \leq (m'_1, \cdots, m'_k) \text{ if, and only if, } m_i \leq m'_i \text{ for every } i.$$

(2.3) *The lattice of the subgroups of the group G is lattice isomorphic with the lattice $L(n_1, \cdots, n_k)$ if, and only if,*

(a) *G is a finite cyclic group;*

(b) *the order of G is $\prod_{i=1}^{k} p_i^{n_i}$ where the p_i are suitably chosen different prime numbers.*

Proof. If G satisfies the conditions (a) and (b), then the subgroup S of G has an order of the form $\prod_{i=1}^{k} p_i^{m_i}$ with $0 \leq m_i \leq n_i$. Put $S^f = (m_1, \cdots, m_k)$. It is easily verified that f is a lattice-isomorphism of the lattice of the subgroups of G upon the lattice $L(n_1, \cdots, n_k)$.—Suppose now conversely that there exists a lattice-isomorphism g of $L(n_1, \cdots, n_k)$ upon the lattice of the subgroups of G. Then it is a consequence of (2.1) that $G_i = (0, \cdots, 0, n_i, 0, \cdots, 0)^g$ is a cyclic group of prime power order $q_i^{n_i}$ and that the subgroup $(m_1, \cdots, m_k)^g$ is cyclic of prime power order if, and only if, at most one of the integers m_i is $\neq 0$. Thus an element x in G is of prime power

order if, and only if, x is contained in one of the groups G_i. If g_i generates G_i, then $g = \prod_{i=1}^{k} g_i$ is not contained in any of the groups $(n_1, \cdots, n_{i-1}, n_i - 1, n_{i+1}, \cdots, n_k)^g$. Since these subgroups of G are just all the greatest subgroups $\neq G$ of G, it follows that g generates G. Thus G is a cyclic group of finite order. This implies that the prime numbers q_i are different, since all the subgroups of a cyclic group are cyclic, and thus the order of G is $\prod_{i=1}^{k} q_i^{n_i}$.

An obvious consequence of (2.3) is the

THEOREM 2.4. *Suppose that G is a cyclic group of order $\prod_{i=1}^{k} p_i^{n_i}$, where the p_i are different prime numbers. Then G and the group H are subgroup-isomorphic if, and only if, H is a cyclic group of order $\prod_{i=1}^{k} q_i^{n_i}$ where the q_i are suitably chosen different prime numbers.*

COROLLARY 2.5. *A subgroup-isomorphism of the finite cyclic group G is induced by an isomorphism of G if, and only if, it is index-preserving.*

In conclusion it may be mentioned that automorphisms of finite cyclic groups induce the identity in the lattice of subgroups and that the identity is the only subgroup-automorphism of a cyclic group of prime power order. But if p and q are different prime numbers, then there exists a subgroup-automorphism of the cyclic group of order pq which interchanges the subgroup of order p and the subgroup of order q.

3. Infinite cyclic groups.

(3.1) *The group G is an infinite cyclic group if, and only if, there exists a one-one-correspondence f between the positive integers and the subgroups $\neq 1$ of G such that*

$$n \text{ is a multiple of } m \text{ if, and only if, } n^f \leq m^f \leq G.$$

Proof. If G is an infinite cyclic group, then a correspondence f which meets the requirements of the theorem is defined in mapping the positive integer n upon the uniquely determined subgroup of index n in G.

Suppose now that there exists a correspondence f between the positive integers and the subgroups $\neq 1$ of the group G which meets the requirements of the theorem. If $x \neq 1$ is an element in G, then denote by $n(x)$ the uniquely determined positive integer such that $n(x)^f$ is generated by x. Since every subgroup $\neq 1$ of G contains an infinity of subgroups, every $n(x)^f$ for

$x \neq 1$ is an infinite cyclic subgroup of G. If x and y are two elements $\neq 1$ in G, then denote by $m(x, y) = m$ the l. c. m. of $n(x)$ and $n(y)$ and by $d(x, y)$ the g. c. d. of $n(x)$ and $n(y)$. It is a consequence of the properties of f, that $m(x, y)^f$ is the meet of the two infinite cyclic subgroups $n(x)^f$ and $n(y)^f$ and that $d(x, y)^f$ is the subgroup of G which is generated by x and y. As $m(x, y)^f$ is $\neq 1$ and the meet of two infinite cyclic subgroups, it is itself an infinite cyclic subgroup of G, and as $m(x, y)^f$ is generated by a power of x which equals a power of y, it follows that $m(x, y)^f$ is contained in the central of $d(x, y)^f$. This implies that $m(x, y)^f$ is a normal subgroup of $d(x, y)^f$ and now it is a consequence of (2. 3) that $d(x, y)^f/m(x, y)^f$ is a cyclic group. Thus the central quotient group of $d(x, y)^f$ is cyclic and this implies that $d(x, y)^f$ is abelian. Hence x and y are permutable and this proves:

G is abelian.

Since there exists only a finite number of subgroups of G which contain a given subgroup $\neq 1$ of G—for n^f is only contained in those m^f with $n = n'm$—it follows that every set of subgroups of G contains some greatest subgroup. Hence there exists a greatest cyclic subgroup of G. If z generates such a greatest cyclic subgroup of G, and if x is any element $\neq 1$ in G, then there exist relatively prime integers h and k such that

$$z^h = x^k \neq 1$$

since all the elements $\neq 1$ in G are of infinite order, and since the meet of any two infinite cyclic subgroups of G is an infinite cyclic subgroup. There exist furthermore integers h', k' such that $hh' + kk' = 1$ and consequently:

$$z = z^{hh'+kk'} = z^{kk'}x^{kh'} = (z^{k'}x^{h'})^k \text{ as } G \text{ is abelian.}$$

But since $n(z)^f$ is a greatest cyclic subgroup of G, and since all the elements $\neq 1$ in G are of infinite order, it follows that $k = \pm 1$ and z consequently generates G, i. e. G is an infinite cyclic group.

An obvious inference from (3. 1) is

THEOREM 3. 2. *The infinite cyclic group G and the group H are subgroup-isomorphic if, and only if, H is an infinite cyclic group.*

A consequence of Theorem 3. 2 and Corollary 2. 5 is the

COROLLARY 3. 3. *A subgroup-isomorphism f of the infinite cyclic group G is induced by an isomorphism of G if, and only if, f is index-preserving.*

Remark. The group of the subgroup-automorphisms of the infinite cyclic group G is isomorphic with the group of all the permutations of the set of all the prime numbers. But the automorphisms of G induce the identical subgroup-automorphism.

4. Ideal-cyclic groups. A group G is called *ideal-cyclic,* if every finite subset of G is contained in some cyclic subgroup of G. Since cyclic groups are abelian, and since therefore any pair of elements in an ideal-cyclic group is contained in an abelian group, it follows that

ideal-cyclic groups are abelian.

Since the elements $\neq 1$ in a cyclic group are either all of infinite order or are all of finite order, it follows that the elements $\neq 1$ in an ideal-cyclic group are either all of infinite order or are all of finite order.

(4. 1) *If G is an ideal-cyclic group and if H is subgroup-isomorphic with G, then H is ideal-cyclic.*

Proof. If $\mathfrak{f}$ is a subgroup-isomorphism of H upon G, and if F is a subgroup of H which is generated by a finite number of elements, then it is a consequence of Theorems 2. 4 and 3. 2 that $F^{\mathfrak{f}}$ is generated by a finite number of elements. Since G is ideal-cyclic, $F^{\mathfrak{f}}$ is contained in a cyclic subgroup of G and therefore itself cyclic. Now it follows from the Theorems 2. 4 and 3. 2 that F is a cyclic subgroup of H and this proves that H is ideal-cyclic.

If the group R contains elements of order p, then the prime-number p is said to be *relevant* for the group R.

THEOREM 4. 2. *The ideal-cyclic group G without elements of infinite order and the group H are subgroup-isomorphic if, and only if,*

(a) *H is an ideal-cyclic group without elements of infinite order;*

(b) *there exists a one-one-correspondence $\mathfrak{r}$ between the prime numbers which are relevant for G and those which are relevant for H such that*

G contains elements of order p^n if, and only if, H contains elements of order $(p^{\mathfrak{r}})^n$.

Proof. Suppose that $\mathfrak{f}$ is a subgroup-isomorphism of G upon H. Then H is by (4. 1) an ideal-cyclic group. If x is any element, then denote by $\bar{x}$ the subgroup, generated by x. If u is an element of prime power order p^n, then $\bar{u}^{\mathfrak{f}}$ is by (2. 2) a cyclic group of prime power order p'^n. If v is an element of prime power order q^m, then $\bar{v}^{\mathfrak{f}}$ is of order q'^m. If $p \neq q$, then uv is of

order $p^n q^m$, $\overline{uv}^f$ of order $p'^n q'^m$ and it follows from Theorem 2.4 that $p' \neq q'$. Now (b) is a consequence of the fact that f^{-1} is a subgroup-isomorphism of the ideal-cyclic group H upon G.

Assume now that the conditions (a) and (b) are satisfied. If the prime number p is relevant for G, then the p-component G_p of G is either a cyclic group of order $p^{n(p)}$ or a group [5] of type p^∞. If f is the correspondence between the relevant prime numbers which enters into condition (b), then the p^f-component H_{p^f} of H is correspondingly either a cyclic group of order $(p^f)^{n(p)}$ or of type $(p^f)^\infty$. Now it is obvious how to extend the correspondence f between the relevant prime numbers to a subgroup-isomorphism of G upon H which always maps G_p upon H_{p^f}.

THEOREM 4.3. *Suppose that G is an ideal-cyclic group without elements $\neq 1$ of finite order. Then G and the group H are subgroup-isomorphic if, and only if,*

(a) *H is an ideal-cyclic group without elements $\neq 1$ of finite order;*

(b) *to every infinite cyclic subgroup Z of G there exists an infinite cyclic subgroup Z' of H such that*

(b′) *G/Z and H/Z' are subgroup-isomorphic;*

(b″) *the number of prime numbers which are not relevant for G/Z is the same as the number of prime numbers which are not relevant for H/Z'.*

Proof. If f is a subgroup-isomorphism of G upon H, then H is ideal-cyclic as follows from (4.1). If Z is an infinite cyclic subgroup of G, then it follows from Theorem 3.2 that $Z' = Z^f$ is an infinite cyclic subgroup of H. As H is abelian, it follows that f induces a subgroup-isomorphism between the quotient groups G/Z and H/Z'.

Since there is no subgroup between Z and Z^p, if p is a prime number, the index of $(Z^p)^f$ in Z' is a uniquely determined prime number p^g and g is a permutation of the prime numbers, since both f and f^{-1} are subgroup-isomorphisms. If p is a relevant prime number for G/Z, then there exists a subgroup $Z(p)$ such that $Z(p)^p = Z$. $Z(p)$ is a uniquely determined infinite cyclic subgroup between G and Z. $Z(p)/Z^p$ is a cyclic group of order p^2 and it follows now from (2.2) that $Z(p)^f/(Z^p)^f$ is a cyclic group of order $(p^g)^2$, since it contains Z'/Z'^{p^g}. Thus g maps primes which are relevant for G/Z

[5] A group G has been defined (by H. Prüfer) as a group of type $p\infty$, if G is generated by an infinite sequence $a(i)$ of elements so that $a(0)$ is of order p and $a(i+1)^p = a(i)$ for every i.

upon primes which are relevant for H/Z' and conversely. This proves the necessity of the conditions (a) and (b).

Assume now that the groups G and H satisfy the conditions (a) and (b). Let Z be an infinite cyclic subgroup of G and Z' an infinite cyclic subgroup of H so that Z and Z' satisfy (b′) and (b″). As G and H are ideal-cyclic groups, it follows that G/Z and H/Z' are ideal cyclic groups without elements of infinite order. Thus there exists by Theorem 4.2 a permutation g of the prime numbers with the property:

the p-component of G/Z and the p^g-component of H/Z' are subgroup-isomorphic.

If X is an infinite cyclic subgroup of G, then both the meet $Z \frown X$ and the join ZX of X and Z are infinite cyclic subgroups of G. If $\prod_p p^{m(X,p)}$ is the index of $Z \frown X$ in Z and $\prod_p p^{j(X,p)}$ is the index of Z in ZX, then there exists one and only one infinite cyclic subgroup X^f of H such that the index of $Z' \frown X^f$ in Z' is $\prod_p (p^g)^{m(X,p)}$ and such that the index of Z' in $Z'X^f$ *is* $\prod_p (p^g)^{j(X,p)}$. f is a one-one-correspondence between the infinite cyclic subgroups of G and the infinite cyclic subgroups of H which preserves meet and join. Thus there exists one and only one subgroup-isomorphism of G upon H which induces f in the set of infinite cyclic subgroups and this completes the proof.

A consequence of the Theorems 4.2 and 4.3 is the

COROLLARY 4.4. *The subgroup-isomorphism f of the ideal-cyclic group G is induced by an (element-)isomorphism of G if, and only if, f is index-preserving.*

5. Groups all of whose elements are of order 2.

LEMMA 5.1. *If all the elements $\neq 1$ of the group G are of order 2, then every subgroup-isomorphism of G is induced by an (element-)isomorphism of G, provided G is not a cyclic group.*

Proof. Since all the elements $\neq 1$ in G are of order 2, G is an abelian group and a direct product of cyclic groups of order 2. Since G is not a cyclic group, G contains at least two independent elements of order 2. If u and v are two elements of order 2 in G, then they are dependent if, and only if, they are equal. If u and v are independent elements, then u is the only element $\neq 1$ in the subgroup $\bar{u}$, generated by u, and uv generates the only proper subgroup of the group, generated by u and v, which is different from $\bar{u}$ and $\bar{v}$.

Assume now that f is a subgroup-isomorphism of G upon the group H. Then every element in H is of order a prime number, as follows from (2.2).

Let u and v be two independent elements $\neq 1$ in G and u' and u'' be elements $\neq 1$ in $\bar{u}^f$, v' an element $\neq 1$ in $\bar{v}^f$. Then both $u'v'$ and $u''v'$ generate $\overline{uv}^f$ and $u'u''v'$ generates the same group as v'. Thus $u'u'' = 1$ and this shows that $\bar{u}^f$ contains exactly one element $\neq 1$. Thus all the elements in H are of order 2 and $u'v'$ is the only element $\neq 1$ in $\overline{uv}^f$. An isomorphism $\mathbf{g}$ of G upon H which induces f is therefore defined by

$$1^g = 1;\text{ if } u \neq 1, \text{ then } u^g \text{ is the uniquely determined element } \neq 1 \text{ in } \bar{u}^f.$$

Remarks. 1. That the Lemma would not be true, if G would be cyclic is a consequence of (2.2). 2. The following example shows that the Lemma does not hold true for direct products of a cyclic group of order 2 and a cyclic group of order 2^n with $2 < n$.

Let H be the group, generated by the two elements u and v which satisfy the relations:

$$1 = u^2 = v^{2^n}, \qquad uvu^{-1}v^{-1} = v^{2^{n-1}}.$$

Then v generates a normal subgroup of order 2^n and $uv^2 = v^2u$ so that u and v^2 generate a subgroup which is a direct product of a cyclic group of order 2 and of a cyclic group of order 2^{n-1}. The only subgroups of H which are not contained in this subgroup are H and the two cyclic groups which are generated by v and uv and these latter ones are just the two cyclic subgroups of order 2^n.

Let now G be the direct product of a cyclic group of order 2 which is generated by an element r and of a cyclic group of order 2^n which is generated by an element s. Then there exists a subgroup-isomorphism of G upon H which maps the cyclic group, generated by r^is^j upon the cyclic subgroup of H which is generated by u^iv^j. This subgroup-isomorphism is index-preserving though H is not even an abelian group.

(The following formula is used in the proof of the facts concerning H which have been mentioned above and this formula shows the point where the assumption $2 < n$ has been needed:

$$(uv)^{2i} = v^{2i(1+2^{n-2})}, \qquad (uv)^{2i+1} = uv^{1+2i(1+2^{n-2})}.)$$

6. Primary hamiltonian groups.

THEOREM 6.1. *Every subgroup-isomorphism of a primary hamiltonian group is induced by exactly four (element-)isomorphisms.*

Proof. It is known [6] that a primary hamiltonian group G is a direct

[6] Cp. e.g. R. Baer, *op. cit.* [3], section 3.

product of a quaternion group and of any number of cyclic groups of order 2. Thus $G = Q \times T$ where the elements $\neq 1$ in T are all of order 2 and where Q is a quaternion group which is generated by two elements u and v satisfying the relations:

$$1 = u^4 = v^4, \qquad u^2 = v^2 = (uv)^2.$$

If g is an automorphism of G which maps every subgroup of G upon itself, i. e. which induces the identical subgroup-automorphism, then

$$t = t^g \text{ for } t \text{ in } T, \quad u^g = u^e, \quad v^g = v^d \text{ with } e^2 = d^2 = 1$$

and all these four possibilities are actually realized by automorphisms of G which induce the identical subgroup-isomorphism. Subgroup-isomorphisms of G which are induced by isomorphisms of G are consequently induced by exactly four isomorphisms of G.

Suppose now that f is a subgroup-isomorphism of G upon the group H. If Q' is the subgroup of Q which is generated by u^2, then Q' is a cyclic subgroup of order 2 and is the meet of the two cyclic subgroups of order 4 which are generated by u and by v. Thus Q^f is generated by two elements which generate cyclic groups, containing Q'^f. Q'^f is therefore contained in the central of Q^f and is consequently a normal subgroup of Q^f. Q/Q' is a direct product of two cyclic groups of order 2 and it follows now from Lemma 5. 1 that Q/Q' and Q^f/Q'^f are isomorphic, since f induces a subgroup-isomorphism of Q/Q' upon Q^f/Q'^f which is by Lemma 5. 1 induced by an isomorphism. If $\bar{u}$ is the cyclic group, generated by u, then this implies that $\bar{u}^f/Q'^f$ is a cyclic group of order 2. It follows therefore from (2. 2) that $\bar{u}^f$ is a cyclic group of order 4, that Q'^f is a cyclic group of order 2. If F is any cyclic subgroup of order 4 of G, then $Q' < F$ and it follows from (2. 2) that F^f is a cyclic group of order 4.

The elements of order 2 in G form exactly the subgroup $Q' \times T$. As it has been proved that Q'^f is a cyclic group of order 2, and as all the elements $\neq 1$ in $Q' \times T$ are of order 2, it follows from Lemma 5. 1 that there exists exactly one isomorphism g of $Q' \times T$ which induces f in $Q' \times T$.—As Q/Q' and $G/(Q' \times T)$ are essentially the same groups, it follows from previous remarks that there exists exactly one isomorphism of $G/(Q' \times T)$ which induces f, as $(Q' \times T)^f$ is exactly the subgroup of all the elements of prime number order in H.

The orders of the elements in H are therefore 2 and 4 and if h is an element of order 4 in H, then h^2 is the only element $\neq 1$ in Q'^f, i. e. $(u^2)^g = h^2$.

Denote now by u' any element, generating $\bar{u}^f$, and by v' any element, generating $\bar{v}^f$. Then it is a consequence from our previous remarks that u' and v' generate H mod $(Q' \times T)^f$, and that u' and v' are independent mod $(Q' \times T)^f$. u', v' and $u'v'$ are therefore elements of order 4 which satisfy:

$$u'^2 = v'^2 = (u'v')^2 = (u^2)^g$$

and this implies that the group Q^f which is generated by u' and v' is a quaternion group.

Every element in G may be represented in one and only one way in the form:

$$u^r v^s x \text{ with } 0 \leq r,s \leq 1 \text{ and } x \text{ in } Q' \times T$$

and it follows from the facts, proved thus far, that a one-one-correspondence between the elements of G and the elements of H is defined by

$$(u^r v^s x)^g = u'^r v'^s x^g.$$

g is clearly an isomorphism in Q and in $Q' \times T$ and induces f in these subgroups of G. But since $(Q' \times T)^f$ is contained in the central of H,—for $u'^2 = u'xu'x$ or $u' = xu'x$ or $u'x = xu'$ and $v'x = xv'$—this implies that g is an isomorphism in the whole group G and g induces f, since ux generates the only cyclic subgroup of order 4 which is contained in the subgroup, generated by u and x, and is not generated by u, if x is not in $\bar{u}$. This completes the proof.

7. Normal subgroup-isomorphisms of abelian and hamiltonian groups.

THEOREM 7. 1. *If f is a normal subgroup-isomorphism of the group G upon the group H, then H is abelian, if G is abelian, and H is hamiltonian, if G is hamiltonian.*

Proof. If all the subgroups of the group G are normal subgroups, and if f is a normal subgroup-isomorphism of G upon H, then all the subgroups of H are normal subgroups. G is hamiltonian if, and only if, all its subgroups are normal and it contains a quaternion group.[7] Now our Theorem is a consequence of Theorem 6. 1, since this Theorem implies that subgroup-isomorphisms map quaternion groups upon quaternion groups.

Remark. In Remark 2 of section **5**, an example of a subgroup-isomorphism of an abelian group upon a non-abelian group has been constructed, so that the assumption of normality cannot be omitted in Theorem 7. 1.

---

[7] Cp. [6].

8. Abelian groups without elements of composite order.

THEOREM 8.1. *Suppose G is a non-cyclic, abelian group, that all its elements $\neq 1$ have the same finite order p, and that the group H satisfies at least one of the following conditions:*

(i) *H is abelian.*

(ii) *All the elements $\neq 1$ in H have the same order.*

(iii) *The group-unit is the only element in H whose order is smaller than p.*

Then G and H are (element-)isomorphic if, and only if, they are subgroup-isomorphic.

Proof. Since every element-isomorphism induces a subgroup-isomorphism we need only prove the sufficiency of the condition.—Since all the elements $\neq 1$ in G have the same finite order p, and since $G \neq 1$, this number p is a prime number. If there exists a subgroup-isomorphism f of G upon H, then it follows from (2.2) that all the elements in H are of prime number order.

Let now u and v be two independent elements in G, W the subgroup, generated by u and v. Then W is a direct product of two cyclic groups of order p, a basis of W is formed by u and v, every proper subgroup of W is a cyclic group of order p and the number of proper subgroups of W is $p+1$.

Assume now that H is abelian. Then W^f is abelian and generated by two elements whose orders are prime numbers. If the orders of these generating elements would be different, then W^f would be a cyclic group. But this is impossible since W is not a cyclic group, as follows from Theorem 2.4. Thus all the elements $\neq 1$ in W^f have the same prime number order q. Since W^f is abelian, this implies that the number of proper subgroups of W^f is $q+1$ and hence $p = q$. Thus it follows that all the elements of the abelian group H are of order p since G is not a cyclic group and therefore contains two independent elements. Since G is a direct product of cyclic groups of order p, and since f preserves this decomposition as H is abelian, it follows that G and H are isomorphic.

Assume next that H satisfies (ii). Then all the elements $\neq 1$ in W^f have the same prime number order q. Since W^f contains but a finite number of subgroups it is finite, and the order of W^f is some power of q. Now it follows from a well known theorem that the central C of W^f is $\neq 1$. Since C is a normal subgroup of W^f and since $W/(C^{f^{-1}})$ is a cyclic group, it follows from Theorem 2.4 that W^f/C is a cyclic group. Since C is the central of W^f, this implies $C \doteq W^f$ and W^f is consequently abelian. Hence any pair of elements

in H is contained in some abelian subgroup of H and this proves that H is abelian. But it has been proved before that this implies isomorphy of G and H.

Assume finally that H satisfies (iii). All the elements of W^f have prime number order. Let V be a cyclic subgroup $\neq 1$ of W^f whose order q is as small as possible. Then (iii) implies $p \leq q$. Denote by N the normalizer of V in $W^f = W'$. Since N lies between the cyclic subgroup $V \neq 1$ and W', there are but two possibilities:

Case 1. $V = N$.

If w is any element in W' but not in V, then w does not transform V into itself. Since w is an element of prime number order r, it follows that w transforms V into r different subgroups which are all different from the subgroup, generated by w. Thus $r + 1 \leq p + 1$ and consequently by the choice of V:

$$p \leq q \leq r \leq p.$$

W' satisfies therefore (ii) and it follows from what has been proved before that W and W' are isomorphic. Hence W' is abelian and W' itself would be the normalizer of V in W' in contradiction to our assumption for this case 1.

Case 2. $W' = N$.

This implies that V is a normal subgroup of W', and since $W/V^{f^{-1}}$ is a cyclic group of prime number order p, it follows from (2.2) that W'/V is a cyclic group of prime number order r. If w is an element in W' but not in V, then w generates W' mod V and r is the order of w. Hence $q \leq r$. The order of the automorphism which w induces in V is either 1 or r and would in the latter case be a divisor of $q - 1$, as V is a cyclic group of prime number order q. But this would contradict $q \leq r$ and w is therefore permutable with the elements in V. This shows that W' is abelian, and from this fact it follows again that H is abelian and that G and H are isomorphic. This completes the proof of our Theorem.

Corollary 8. 2. *Suppose that G is a non-cyclic, abelian group whose elements $\neq 1$ are all of the same finite order, and that f is a subgroup-isomorphism of G upon the group H. Then the following three properties are equivalent:*

(i) *G and H are isomorphic.*

(ii) *f is normal.*

(iii) *f is index-preserving.*

This is a consequence of Theorem 8. 1 and Theorem 7. 1.

Remarks. 1. The existence of an isomorphism between G and H which induces f cannot be proved, since there exist subgroup-automorphisms of direct products of cyclic groups of order $p \neq 2$ which are not induced by element-automorphisms.[8]

2. That the conditions (i), (ii) or (iii) in Theorem 8.1 cannot be omitted, follows from the *existence*[9] *of non-abelian groups which are subgroup-isomorphic with a direct product of two cyclic groups of prime number order* $p \neq 2$.

Let q be a prime number, dividing $p-1$ (e.g. $2 = q$) and let n be an integer such that $0 < n < p$ and such that the multiplicative order of $n \bmod p$ is q (If $q = 2$, then one may choose $n = p - 1$). Let H be the group, generated by two elements u and v, which satisfy the relations:

$$1 = u^p = v^q, \qquad vuv^{-1} = u^n.$$

H is an extension of the cyclic group of order p which is generated by u by a cyclic group of order q, and it is well known that H is essentially the only non-cyclic group of order pq.

The elements in H are all of the form: $u^i v^j$ with $0 \leq i < p$, $0 \leq j < q$ where the numbers i and j are uniquely determined by the element. If $j \neq 0$ and k is a positive integer, then

$$(u^i v^j)^k = u^{if} v^{jk} \text{ where } f = (n^{jk} - 1)(n^j - 1)^{-1}$$

and the order of $u^i v^j$ is q, if $j \neq 0$. Furthermore it may be inferred from this formula that every cyclic subgroup of H which is not generated by a power of u contains one and only one element of the form: $u^i v$. Since every proper subgroup of H is a cyclic group of prime number order, this shows that H contains exactly $p + 1$ proper subgroups, and that consequently H is subgroup-isomorphic with the direct product of two cyclic groups of order p.

(8.3) *If the group H is subgroup-isomorphic with a direct product of two cyclic groups of prime number order p, then H contains an element of order p.*

Proof. H contains exactly $p + 1$ proper subgroups and every proper subgroup of H is a cyclic group whose order is some prime number. Let Z be some cyclic subgroup $\neq 1$ of H and let the prime number r be its order, z an element which generates Z.

---

[8] Cp. e. g. the Remark at the end of section 11.

[9] This example could be obtained as a special case of Theorem 11.2.

Case 1. There does not exist a proper subgroup $X \neq Z$ of H so that

$$zXz^{-1} = X.$$

In this case each of the p proper subgroups $X \neq Z$ is transformed by the elements in Z into exactly r different conjugate subgroups $\neq Z$, as r is a prime number. Consequently p is a multiple of r and this implies $p = r$, i. e. z is an element of order p.

Case 2. There exists a subgroup $W \neq 1$ of prime number order which is transformed into itself by the elements in Z.

Since H is generated by Z and W, it follows that W is a normal subgroup of H. Consequently H/W is a cyclic group of prime number order r. If q is the order of W, then rq is the order of H. If $q = r$, then $q = r = p$ by Theorem 8. 1. If $q \neq r$, then—as $q \neq r$ and Theorem 8. 1 imply that H is not abelian—r is a divisor of $q - 1$ and H is of the type discussed in Remark 2 just above. In particular the number of proper subgroups of H is $q + 1$ and this implies $q + 1 = p + 1$, $q = p$. Hence W is of order p and this completes the proof.

9. Element-functions, derived from subgroup-isomorphisms.[10] The following *notation* will be used throughout: $\{\ldots\}$ is the subgroup, generated by the element sets inside the brackets.

(9. 1) *If G is the direct product of the cyclic groups X and Y, if f is a subgroup-isomorphism of G upon the group H, if $X^f = \{x'\}$ and $Y^f = \{y'\}$, then $Z = \{x'y'\}^{f^{-1}} = \{xy\}$ where x generates X and y generates Y.*

Proof. That Z is a cyclic subgroup of G, is a consequence of the Theorems 2. 4 and 3. 2. Hence Z is generated by an element of the form xy where x is an element in X and y in Y. If x would not generate X, then Z would be a subgroup of $X'Y$ where $X' = \{x\}$ is a proper subgroup of X. This would imply that x' is an element of X'^fY^f, that $X^f \leq X'^fY^f$ and that consequently $X \leq X'Y$. But this is impossible and consequently $X = \{x\}$, $Y = \{y\}$.

(9. 2) *Suppose that f is a subgroup-isomorphism of the abelian group G upon the group H, that x and u are independent elements in G and that $\{u\}^f = \{u'\}$.*

(a) *If u is of infinite order, then there exists one and only one element $x' = f(x; u, u', f)$ so that*

[10] The methods evolved in this section seem to admit of an extension to certain classes of abelian operator groups.

(9. F) $$\{x\}^f = \{x'\}, \qquad \{xu\}^f = \{x'u'\}.$$

(b) *If x and u are of finite order, and if the order of u is a multiple of the order of x, then there exists at most one solution x' of the pair* (9. F) *of functional equations.*

(c) *If u' transforms $\{x\}^f$ into itself and if the order of u is* [*either infinite or*] *a multiple of the order of x, then there exists at least one solution x' of* (9. F).

(d) *If the order of u is finite and a multiple of the order of x, and if the number of elements, generating $\{x\}$, is not greater than the number of elements which generate $\{x\}^f$, then there exists one and only one element $x' = f(x; u, u', f)$, satisfying* (9. F).

Proof. Suppose that the elements x' and x'' are both solutions of (9. F). Assume first that u is of infinite order. Then either $x'u' = x''u'$ which implies $x' = x''$; or $x'u' = (x''u')^{-1}$. In the latter case we would have: $(x'u')^2 = x'u'u'^{-1}x''^{-1} = x'x''^{-1}$. But since $\{xu\}$ and $\{x\}$ have only the group-unit in common, we would have in this case $x'x''^{-1} = 1$ or $x' = x''$.—If secondly u is an element of finite order, then there exists a positive integer k so that $x'u' = (x''u')^k = x''(u'x'')^{k-1}u'$ or $x''^{-1}x' = (u'x'')^{k-1}$, since xu is an element of finite order too. Since under the assumptions of (b) the group-unit is the only element in common to $\{x\}$ and $\{xu\}$, it follows from (9. 1) that $x''^{-1}x' = 1$ or $x'' = x'$.

If u' transforms $\{x\}^f$ into itself, then denote by y any element, generating $\{x\}^f$. Every element of $\{y, u'\}$ has the form $y^iu'^j$ and $(y^iu'^j)^k = y^tu'^{jk}$. Thus $\{xu\}^f = \{y^iu'^j\}$ and it is a consequence of (9. 1) that u'^j generates $\{u'\}$. Since $\{x\}$ and $\{xu\}$ have only the group-unit in common, it follows that u', u'^j and $y^iu'^j$ have the same order. Thus there exists an integer k such that $u' = u'^{jk}$ and $\{y^iu'^j\} = \{(y^iu'^j)^k\}$. If $(y^iu'^j)^k = y^su'^{jk} = y^su'$, then it is a consequence of (9. 1) that y^s generates $\{y\}$ and this proves (c).

Assume now that the number of elements which generate $\{x\}$ is not greater than the number of elements which generate $\{x\}^f$ and that u is either of infinite order or of an order which is a multiple of the order of x. Then it follows from what has been proved above that the number of subgroups of the form $\{vu'\}$ with $\{v\} = \{x\}^f$ is exactly equal to the number of elements v which generate $\{x\}^f$ and it is a consequence of (9. 1) that each of these subgroups satisfies: $\{vu'\}^{f^{-1}} = \{wu\}$ with $\{w\} = \{x\}$. Since the number of subgroups of the form $\{wu\}$ with $\{w\} = \{x\}$ is finite, it follows that these two numbers of subgroups are equal and that every $\{wu\}^f$ is of the form $\{vu'\}$.

Thus everything has been proved except the existence-assertion in (a). But if x is an element of finite order, then $\{x\}^f$ is the subgroup of all the elements of finite order of $\{x, u\}^f$ as u is of infinite order. Hence $\{x\}^f$ is a cyclic normal subgroup of $\{x, u\}^f$ and (c) may be applied.—If x is of infinite order, then $\{x\}^f$ is by Theorem 3. 2 a cyclic group of infinite order and $\{x\}$ and $\{x\}^f$ have both exactly two generating elements so that the result may be applied which has been derived in the last paragraph. This completes the proof.

Remark. The example given in Remark 2 of section **8** shows that the additional hypothesis in (c) and (d) cannot be omitted.

COROLLARY 9. 3. *If the element u and the subgroup S of the abelian group G are independent if $u^i = 1$ implies $S^i = 1$, if $\mathfrak{f}$ is a subgroup-isomorphism of G upon the group H, if u' is an element in H so that $\{u\}^{\mathfrak{f}} = \{u'\}$, and if there exists to every element x in S one and only one solution $x' = f(x; u, u', \mathfrak{f})$ of* (9. F), *then $f(x; u, u', \mathfrak{f})$ constitutes a one-one-correspondence between the elements of S and the elements of $S^{\mathfrak{f}}$ which induces $\mathfrak{f}$.*

Proof. If y is any element in $S^{\mathfrak{f}}$, then it follows from (9. 1) that there exist elements z and v so that $\{z\}^{\mathfrak{f}} = \{y\}$, $\{v\}^{\mathfrak{f}} = \{u'\}$ and $\{zv\}^{\mathfrak{f}} = \{yu'\}$. Since v and u consequently generate the same subgroup, it follows that there exists some integer $k \neq 0$ so that $v^k = u$. Since $u^i = 1$ implies $z^i = 1$, it follows that z and z^k generate the same subgroup, and as G is abelian it follows that zv and $(zv)^k = z^k u$ generate the same subgroup. Hence $y = f(z^k; u, u', \mathfrak{f})$ and f maps S upon the whole group $S^{\mathfrak{f}}$. Since f and $\mathfrak{f}$ coincide on the cyclic subgroups of S, this completes the proof.

(9. 4) *If u, v and w are three independent elements in the abelian group G so that $u^i = 1$ implies $v^i = 1$ and $v^k = 1$ implies $w^k = 1$, if $\mathfrak{f}$ is a subgroup-isomorphism of G upon the group H, if u' is an element in H so that $\{u\}^{\mathfrak{f}} = \{u'\}$ and so that there exists to every element x in $\{v, w\}$ one and only element $x' = f(x; u, u', \mathfrak{f})$ which satisfies* (9. F), *then*

$$f(wv; u, u', \mathfrak{f}) = f(w; u, u', \mathfrak{f}) f(v; u, u', \mathfrak{f}).$$

Proof. It is a consequence of the Corollary 9. 3 that $\mathfrak{f}$ is strictly index-preserving on $\{v, w\} = S$. Thus there exists by (9. 2) one and only one element $f(w; v, v', \mathfrak{f}) = w'$ so that $\{w\}^{\mathfrak{f}} = \{w'\}$ and $\{wv\}^{\mathfrak{f}} = \{w'v'\}$ if we put $v' = f(v; u, u', \mathfrak{f})$. Consequently we have:

$$f(wv; u, u', \mathfrak{f}) = f(w; v, v', \mathfrak{f}) f(v; u, u', \mathfrak{f}) [= w'v'].$$

As f is strictly index-preserving on $\{v, w\}$, as vu is independent of S and as $(v^j u)^i = 1$ implies $x^i = 1$ for every x in S, it follows from (9.2) that there exists one and only one element $x' = f(x; vu, (vu)', f)$ so that $\{x\}^f = \{x'\}$ and $\{xvu\}^f = \{x'(vu)'\}$, if only x is an element in S and $(vu)' = v'u'$. This implies $f(w; v, v', f) = f(w; vu, (vu)', f)$. But as u and vu behave symmetrically with regard to S and w and v, this implies $f(w; v, v', f) = f(w; u, u', f)$ and this completes the proof.

(9.5) *Suppose that the abelian group G contains to every element x an element y so that x and y are independent and so that $y^i = 1$ implies $x^i = 1$. If f is a subgroup-isomorphism of G upon the group H, and if $f(x)$ is a one-one-correspondence between the elements of G and the elements of H which induces f and satisfies:*

$f(xy) = f(x)f(y)$, if x and y are independent and $y^i = 1$ implies $x^i = 1$; then f is an isomorphism of G upon H.

Proof. If $x \neq 1$ is any element in G, then there exists in G an element y so that x and y are independent and so that $y^i = 1$ implies $x^i = 1$. If j is any integer, then x^j and y are independent (if $x^j \neq 1$) and $y^i = 1$ implies $x^{ji} = 1$. Consequently

$$\begin{aligned} f(x^j y) &= f(x^j)f(y) \\ &= f(x^{j-1}xy) = f(x^{j-1})f(xy) = f(x^{j-1})f(x)f(y), \end{aligned}$$

since x^{j-1} and xy are independent (if $x^{j-1} \neq 1$) and since $(xy)^i = 1$ implies $y^i = x^i = 1$ and therefore $x^{(j-1)i} = 1$. Thus it follows by complete induction that

$$f(x^j) = f(x)^j \text{ for every } j \text{ and every } x \text{ in } G.$$

Suppose now that x and y are two elements in G which are independent and which have the property that $y^i = 1$ implies $x^i = 1$. Then

$$\begin{aligned} f(y)^{-1}f(x)^{-1} &= (f(x)f(y))^{-1} = f(xy)^{-1} = f((xy)^{-1}) \\ &= f(x^{-1}y^{-1}) \quad (\text{as } G \text{ is abelian}), \\ &= f(x^{-1})f(y^{-1}) = f(x)^{-1}f(y)^{-1} \end{aligned}$$

and consequently

$$f(xy) = f(x)f(y) = f(y)f(x).$$

If x and y are independent elements, then we certainly have

$$f(xy) = f(x)f(y) = f(y)f(x),$$

if at least one of the elements x and y is of infinite order.—If both are of finite order, then assume first that the orders are relatively prime. In this case the order of xy is the product of the orders of x and of y. There exists an element z so that z and xy are independent and so that $z^i = 1$ implies $(xy)^i = 1$. Then x and yz are independent and $(yz)^i = 1$ implies $x^i = 1$, z and y are independent and $z^i = 1$ implies $y^i = 1$. Thus we have

$$\begin{aligned} f(xyz) &= f(xy)f(z) \\ &= f(x)f(yz) = f(x)f(y)f(z) \end{aligned}$$

or

$$f(x)f(y) = f(xy) = f(yx) = f(y)f(x).$$

If the orders of x and y are powers of the same prime number p, then we may assume that the order of y is a multiple of the order of x. Since x and y are independent we have:

$$f(xy) = f(x)f(y) = f(y)f(x).$$

If x and y are independent elements of some finite order, then $x = x(1) \cdots x(h)$, $y = y(1) \cdots y(h)$ where the orders of $x(i)$ and $y(i)$ are powers of the same prime number $p(i)$, $p(i) \neq p(j)$ for $i \neq j$, and where $x(i)$ and $y(i)$ are independent, if both are $\neq 1$. Then

$$\begin{aligned} f(xy) &= f(x(1)y(1) \cdots x(n)y(n)) \\ &= f(x(1)y(1)) \cdots f(x(n)y(n)) \\ &= f(x(1))f(y(1)) \cdots f(x(n))f(y(n)) = f(x)f(y) \\ &= f(y(1))f(x(1)) \cdots f(y(n))f(x(n)) = f(y)f(x) \end{aligned}$$

so that $f(xy) = f(x)f(y) = f(y)f(x)$ has been proved for any pair of independent elements x and y.

If finally x and y are any two elements in G, then $\{x, y\}$ is a direct product of two cyclic groups (one of them may be equal 1). If r and s form a basis of $\{x, y\}$, then r^i, s^j are independent (if $\neq 1$), and $x = r^h s^k$, $y = r^m s^n$. Consequently

$$\begin{aligned} f(xy) &= f(r^{h+m}s^{k+n}) = f(r^{h+m})f(s^{k+n}) = f(r)^{h+m}f(s)^{k+n} \\ &= f(r)^h f(s)^k f(r)^m f(s)^n = f(r^h)f(s^k)f(r^m)f(s^n) = f(x)f(y) \end{aligned}$$

and thus the formula $f(xy) = f(x)f(y)$ has been proved for any pair of elements x and y in G. This completes the proof.

(9.6) *If f is a subgroup-isomorphism of the abelian group G upon the group H, if S is a subgroup of G and t an element in G so that $\{t\}$ and S are in-*

dependent and so that $t^i = 1$ implies $S^i = 1$, if finally $\{s'\} = \{t's't'^{-1}\}$ for every t' in $\{t\}^f$ and every s' in $S^f = S'$, then S^f is abelian.

Proof. If t' is any element so that $\{t\}^f = \{t'\}$, then it follows from our assumptions and from (9.2) that there exists to every element s in S one and only one element $s' = f(s; t, t', f)$ such that

$$\{s\}^f = \{s'\}, \qquad \{st\}^f = \{s't'\}.$$

The elements x and y in $S' = S^f$ are certainly permutable, if they generate a cyclic subgroup. If $\{x, y\}$ is not a cyclic subgroup, then it follows from Theorems 2.4 and 3.2 that $V = \{x, y\}^{f^{-1}}$ is not cyclic. But as V is an abelian group which is generated by two elements, there exists a basis of V which consists of two elements u and v, and the elements u' and v' which have been defined above generate the subgroup $V^f = \{x, y\}$.

From our assumptions concerning t' and S' it follows that

$$t'u't'^{-1} = u'^i,\ \{u'\} = \{u'^i\},\ t'v't'^{-1} = v'^j,\ \{v'\} = \{v'^j\}.$$

Hence

$$v'^{-1}(u't')^{-1}v'(u't') = v'^{j-1}v'^{-j}u'^{-i}v'^ju'^i = v'^{j-1}c',$$
$$(v't')^{-1}u'^{-1}(v't')u' = v'^{-j}u'^{-i}v'^ju'^iu'^{1-i} = c'u'^{1-i}.$$

The first of these equations shows that $v'^{j-1}c'$ is contained in the meet of $\{u't', v'\} = \{ut, v\}^f$ and $\{u', v'\} = \{u, v\}^f$. But the meet of $\{ut, v\}$ and $\{u, v\}$ is $\{v\}$, since $\{t\}$ and S are independent and since $t^k = 1$ implies $S^k = 1$. Consequently both $v'^{j-1}c'$ and c' are elements of $\{v'\}$. By the same argument it follows from the second of the above equations that c' is an element of $\{u'\}$. The meet of $\{u'\}$ and $\{v'\}$ is 1, since u and v are independent elements. Hence $c' = 1$ or $u'^iv'^j = v'^ju'^i$. But this proves that V is abelian, since

$$V = \{x, y\} = \{u', v'\} = \{u'\}\{v'\} = \{u'^i\}\{v'^j\} = \{u'^i, v'^j\},$$

and S' is therefore abelian.

10. The number of isomorphisms inducing a given subgroup-isomorphism. If G is a group and f a subgroup-isomorphism of G, then there is either no isomorphism of G which induces f or the number of isomorphisms of G which induce f is exactly the number of automorphisms of G which map every subgroup of G upon itself, i. e. which induce the identical subgroup-automorphism of G. If G is a primary abelian group, then these automorphisms have been determined before.[11] Here the case shall be discussed where G is an abelian group which contains elements of infinite order.

[11] Reinhold Baer, "Primary abelian groups and their automorphisms," *American Journal of Mathematics*, vol. 49 (1937), pp. 99-117, Theorem 5.2.

(10. 1) *If G is an abelian group, containing elements of infinite order, then the automorphisms:*

$$x = x^{g} \text{ for every } x, \text{ and } x^{-1} = x^{g} \text{ for every } x,$$

are the only automorphisms of G which map every subgroup of G upon itself.

Proof. That the two automorphisms, mentioned in the theorem, have the required properties, is obvious.—If conversely g is an automorphism of G which satisfies $S = S^{g}$ for every subgroup S of G, then there exists to every element x in G a number $n(x)$ such that $x^{g} = x^{n(x)}$ and such that x and $x^{n(x)}$ generate the same subgroup. If u is an element of infinite order in G, then $n(u) = e = \pm 1$. If v is an independent element of u (of finite or infinite order), then

$$\begin{aligned}(uv)^{g} &= u^{n(uv)}v^{n(uv)} \\ &= u^{g}v^{g} = u^{e}v^{n(v)}\end{aligned}$$

and now it follows that $e = n(uv) = n(v)$ mod the order of v, if v is of finite order

$= n(v)$ if v is of infinite order.

This implies $x^{g} = x^{e}$ for every x, and this proves our statement.

11. Abelian groups without elements of infinite order. If G is an abelian group without elements of infinite order, then G is the direct product of its primary components G_p where G_p contains all those elements in G whose order is a power of the prime number p.

(11. 1) *If G is an abelian group without elements of infinite order and if f is a subgroup-isomorphism of G upon the group H, then H is the direct product of its subgroups $G_p{}^{f}$ and the orders of elements in different subgroups $G_p{}^{f}$ are relatively prime.*

Proof. Suppose that $p \neq q$ are prime numbers, that u is an element in $G_p{}^{f}$ and v in $G_q{}^{f}$. Then $\{u\}^{f^{-1}} \leq G_p$ is a cyclic group, generated by u', and $\{v\}^{f^{-1}} = \{v'\} \leq G_q$. Thus $u'v'$ is an element of order $p^{m}q^{n}$ and $\{u'v'\}$ contains the element u' of order p^{m} and the element v' of order q^{n}. It is now a consequence of Theorem 2. 4 that u is of order p'^{m}, v of order q'^{n} and uv of order $p'^{m}q'^{n}$ where p' and q' are different prime numbers. Thus u and v are permutable and this completes the proof.

As a consequence of this statement (11. 1) it will be no loss in generality to assume throughout this section that the abelian group G is a primary group.

THEOREM 11. 2. (a) *There exists a subgroup-isomorphism which is not*

index-preserving of the abelian p-group G which is not ideal-cyclic if, and only if,

(i) $p \neq 2$;

(ii) *G is a direct product of cyclic groups of order p.*

(b) *There exists a subgroup-isomorphism which is not index-preserving of the group H upon an abelian, but not ideal-cyclic p-group if, and only if, there exists a subgroup W of H with the following properties:*

(1) *W is a direct product of cyclic groups of order p;*

(2) $W \neq 1$ *and* $p \neq 2$;

(3) *W is a normal subgroup of H and H/W is a cyclic group of order q where q is a divisor* $\neq 1$ *of* $p-1$, *q a prime number;*

(4) *if w is some element which generates H mod W, then* $w^{-1}xw = x^j$ *for every x in W*

where the integer j does not depend on x and where j is an integer which is relatively prime to p and whose (multiplicative) order mod p is exactly q.

Proof. Assume first that f is a subgroup-isomorphism of the abelian p-group G upon the group H, that f is not index-preserving and that G is not ideal-cyclic. Denote by G^* the subgroup of all the elements of order p in G and put $H^* = G^{*f}$. If all the elements $\neq 1$ in H^* would be of order p, then f would be index-preserving, since a power $\neq 1$ of every element $\neq 1$ in H is contained in H^*, and since by (2.2) all the elements in H are of prime power order. Hence H^* contains elements whose order is a prime number $q \neq p$. Note furthermore that G^* and H^* are not cyclic groups, since G is not ideal-cyclic.

Suppose now that x' and y' are two elements of order p in H^*. If they are dependent, then they generate the same cyclic subgroup of H^*. If they are independent, then $\{x', y'\}^{f^{-1}}$ is a direct product of two cyclic groups of order p. If $\{y'\}$ would not be a normal subgroup of $\{x', y'\}$, then x' would transform $\{y'\}$ in exactly p different subgroups of $\{x', y'\}$ since p is the order of x'. Since the number of proper subgroups of $\{x', y'\}$ is exactly $p+1$, and since the index of every proper subgroup of $\{x', y'\}$ in $\{x', y'\}$ is p and the group of permutations which the inner automorphisms of $\{x', y'\}$ effect in the set of $p+1$ proper subgroups of $\{x', y'\}$ is therefore not transitive, this implies that $\{x'\}$ is transformed by y' into itself and $\{x'\}$ is consequently a normal subgroup of $\{x', y'\}$. Thus at least one of the groups $\{x'\}$ and $\{y'\}$

is a normal subgroup of $\{x', y'\}$ and this subgroup as well as its quotient group—which is represented by the other of the two subgroups—is of order p, and it follows therefore that $\{x', y'\}$ is of order p^2 and that all its elements $\neq 1$ are of order p. Thus it has been proved:

(11. 2. 1) *The elements of order p in H^* form a subgroup W of H^*.*

If $V = W^{f^{-1}}$, then it is a consequence of Theorem 8. 1 that V and W are isomorphic and W is in particular therefore a direct product of cyclic groups of order p. Since all the elements of prime number order in H are contained in H^*, it follows that W is the subgroup of all the elements of order p in H. Thus W is a *normal* subgroup of H.

V is a direct factor of G^*. If G^* is the direct product of V and V', then V'^f and W have only the group unit in common. V'^f contains therefore no elements of order p. Since V' is a direct product of cyclic groups of order p, it follows now from (8. 3) that V' is a cyclic group and this implies:

(11. 2. 2) *H^*/W is a cyclic group of prime number order $q \neq p$.*

Assume now that w is an element of order p^2 in H. Then w^p is an element of order p in W. Let t be some element in H^* which is not contained in W. Then all the results, derived so far, may be applied upon the groups $\{t, w\}^{f^{-1}}$ and $\{t, w\}$. Thus $\{w^p\}$ is the subgroup of all the elements of order p in $\{t, w\}$ and is a normal subgroup of $\{t, w\}$. Hence all the results may be applied upon the groups $\{t, w\}^{f^{-1}}/\{w^p\}^{f^{-1}}$ and $\{t, w\}/\{w^p\}$ and $\{w\}/\{w^p\}$ is therefore the normal subgroup of all the elements of order p of $\{t, w\}/\{w^p\}$. This proves that $\{w\}$ is a normal subgroup of $\{t, w\}$ and that $twt^{-1} = w^j$ for some j prime to p. Thus we have:

$$(wt)^p = w\, twt^{-1}\, t^2wt^{-2} \cdots t^{p-1}wt^{1-p}t^p = w^h t^p \quad \text{with} \quad h = 1 + j + \cdots + j^{p-1}.$$

It is a consequence of (9. 1) that $\{wt\}^{f^{-1}} = \{w't'\}$ with $\{w'\}^f = \{w\}$ and $\{t'\}^f = \{t\}$. Since $\{w'^p\} = \{w', t'\}^p = (\{w, t\}^f)^p$, it follows from (2. 2) that $\{(wt)^p\} = \{w^p\}$ and this together with the above identity would imply $t^p = 1$, as $\{t\}$ and $\{w\}$ are independent. But this is impossible since t is an element of the prime number order $q \neq p$ and therefore the following fact has been proved:

(11. 2. 3) *H does not contain elements of order p^2.*

Denote now by R the meet of G^p and G^*. It is a consequence of (11. 2. 3) that R^f and W have only the unit-element in common. Thus, it follows from (11. 2. 2) that either $R = 1$ or R is a cyclic group of order p and G^* is the

direct product of R and V. If $R \neq 1$, then R^f is the only cyclic subgroup of prime number order of H which is contained in a greater cyclic subgroup. Thus R^f is a normal cyclic subgroup of H. Since H^* is the join of R^f and W, since both these subgroups are normal and have only the group-unit in common, it follows that H^* is their direct product. Since W is abelian and since R and R^f are cyclic, H^* is abelian, and since H^* is not cyclic it would follow from Theorem 8.1 that G^* and H^* are isomorphic. As this is impossible, it follows that $R = 1$, $G = G^*$ and $H = H^*$. From the last argument the following fact may be derived:

(11.2.4) *If t is an element in H which is not contained in W, then $\{t\}$ is a not-normal subgroup of order q of H.*

If t is an element in H, but not in W, $w \neq 1$ is an element in W, then the previous results may be applied upon $\{t, w\}^{f^{-1}}$ and $\{t, w\}$. Consequently $\{w\}$ is a normal subgroup of $\{t, w\}$ and $\{t\}$ is not a normal subgroup of $\{t, w\}$. Hence $twt^{-1} = w^j$ where j is relatively prime to p and where the multiplicative order of j mod p is exactly q. Thus q is a divisor of $p - 1$. Since t induces thus an automorphism of W which maps every subgroup of W upon itself, it follows from known theorems [11] that j is the same for all the elements in W.

Thus the necessity of all the conditions (i), (ii), (1) to (4) has been proved.

In order to prove the sufficiency of these conditions, let p be a prime number $\neq 2$, q a prime number dividing $p - 1$, j an integer, prime to p whose multiplicative order mod p is exactly q, and let $W \neq 1$ be a direct product of cyclic groups of order p. Let H be the group, generated by the elements in W and an element t, satisfying:

$$t^q = 1,\ txt^{-1} = x^j \text{ for every } x \text{ in } W.$$

Every element in H has the form: xt^i with $0 \leq i < q$ and x in W.

$$(xt^i)^k = x\, t^i x t^{-i}\, t^{2i} x t^{-2i} \cdots t^{(k-1)i} x t^{(1-k)i} t^{ki} = x^h t^{ki}$$

with $h = 1 + j^i + j^{2i} + \cdots + j^{(k-1)i}$. Since $j - 1$ is prime to p, h is divisible by p if, and only if, $j^{ik} - 1$ is divisible by p, i. e., $j^{ik} \equiv 1 \bmod p$. If i is relatively prime to q, the order of xt^i is exactly q and there exists exactly one element x' in W so that $\{xt^i\} = \{x't\}$. Thus a one-one-correspondence has been defined between the elements in W and the cyclic subgroups of H which are not contained in W.

Let now G be the direct product of W and of the cyclic group $\{t'\}$ of order p. Then all the cyclic subgroups $\neq 1$ of G are of order p and to every

cyclic subgroup Z of G which is not contained in W there exists one and only one element x in W so that xt' generates Z. There exists a uniquely determined subgroup-isomorphism f of G upon H so that $S^f = S$ for $S \leq W$, $\{xt'\}^f = \{xt\}$ for x in W and this completes the proof of our Theorem.

COROLLARY 11. 3. *If G is an abelian p-group which contains elements of order p^2 and which is not ideal-cyclic, then every subgroup-isomorphism of G is index-preserving.*

COROLLARY 11. 4. *If G is an abelian p-group, but not ideal-cyclic, f a subgroup-isomorphism of G upon the abelian group H, then f is index-preserving.*

Both these Corollaries are consequences of Theorem 11. 2 and its proof.

LEMMA 11. 5. *If G is an abelian p-group so that $G^{p^m} = 1$ whereas $G^{p^{m-1}}$ contains at least p^3 elements $(0 < m)$, then every index-preserving subgroup-isomorphism of G is induced by an (element-)isomorphism of G.*

Proof. Since the orders of the elements in G are bounded, there exists [12] a basis B of G and this basis B contains at least three elements of the maximum-order p^m. Let f be an index-preserving subgroup-isomorphism of G upon the group H. If b is some element of order p^m in B, B' the subgroup of G which is generated by the elements $\neq b$ in B, and b' some element in H so that $\{b\}^f = \{b'\}$, then it follows from (9. 2) that there exists to every element x in B' one and only one element $x' = f(x; b, b', f)$ in H so that

$$\{x\}^f = \{x'\}, \qquad \{xb\}^f = \{x'b'\}.$$

Since B' contains two independent elements of maximum order, it follows from (9. 4) and (9. 5) that $f(x; b, b', f)$ is an isomorphism of B' upon B'^f such that in particular B'^f is abelian.

H is generated by the elements which are contained in the groups $\{x\}^f$ for x in B. If h and k are two elements in B, then it is possible to choose the element b—used in the first paragraph of the proof—in such a way that it is different from both h and k. Consequently $\{h, k\}^f$ is contained in an abelian subgroup of H and this implies that H possesses a permutable set of generators. Hence *H is abelian.*

Since G is the direct product of B' and $\{b\}$, since both b and b' are elements of order p^m and since H is as an abelian group the direct product of B'^f and $\{b\}^f$, it follows that there exists one and only one isomorphism g of G upon H, so that

[12] A proof of this well known theorem may be found e. g. in R. Baer, "Der Kern, eine characteristische Untergruppe," *Comp. Math.*, Bd. 1 (1934), pp. 254-283, Lemma in § 5.

$$b^g = b', \ x^g = f(x; b, b', f) \text{ for } x \text{ in } B'.$$

In order to prove that this isomorphism g induces f note first that every element in G has the form $b^i c$ for c in B'. Since every basis of B' contains at least two elements of maximum-order p^m, it is possible to represent B' as a direct product of a cyclic group $\{z\}$ of order p^m and of a group C which contains the element c. Then it follows as above that there exists to every element y in $\{b, C\}$ one and only one element $y'' = f(y; z, z^g, f)$ so that

$$\{y\}^f = \{y''\}, \qquad \{yz\}^f = \{y''z^g\}.$$

This function $f(y; z, z^g, f)$ is an isomorphism of $\{b, C\}$. In particular, we have therefore

$$\begin{aligned}\{bz\}^f &= \{f(z; b, b', f)b'\} = \{z^g b'\}\\ &= \{f(b; z, z^g, f)z^g\}\end{aligned}$$

and this implies—as $f(\ldots)$ is uniquely determined—that $b' = f(b; z, z^g, f)$. Similarly we find:

$$\begin{aligned}\{bcz\}^f &= \{f(bc; z, z^g, f)z^g\}\\ &= \{f(cz; b, b', f)b'\} = \{(cz)^g b'\} = \{c^g b' z^g\}\end{aligned}$$

and from the uniqueness of $f(\ldots)$ it follows that

$$c^g b' = f(bc; z, z^g, f) = f(b; z, z^g, f) f(c; z, z^g, f) = f(c; z, z^g, f) b'$$

as $f(\ldots)$ is an isomorphism and consequently we have finally:

$$c^g = f(c; z, z^g, f).$$

Now we find

$$\begin{aligned}\{b^i c\}^f &= \{f(b^i c; z, z^g, f)\} = \{f(b; z, z^g, f)^i f(c; z, z^g, f)\} = \{b'^i c^g\}\\ &= \{(b^i c)^g\}\end{aligned}$$

and this completes the proof.

COROLLARY 11. 6. *If G is an abelian p-group so that $G^{p^m} = 1$ for $0 < m$ but $G^{p^{m-1}}$ contains at least p^3 elements, if f is an index-preserving subgroup-isomorphism of G upon the group H, if u is an element of order p^m in G and u' an element in H so that $\{u\}^f = \{u'\}$, then there exists one and only one isomorphism of G upon H which induces f and maps u upon u'.*

Proof. As a consequence of the Theorem 11. 5 there exists an isomorphism h of G which induces f. Consequently $\{u^h\} = \{u\}^f = \{u'\}$ and there exists therefore an integer j prime to p so that $u^{hj} = u'$. The isomorphism $x^g = x^{hj}$ of G upon H induces f and maps u upon u'.—If g' is another isomorphism which induces f and maps u upon u', then it follows that $g^{-1}g'$ induces the identical subgroup-automorphism in H; consequently $x^{g'} = x^{gi}$

for every x in G and an integer j which is prime to p and does not depend on x. But $u' = u^{\mathbf{g}'} = u^{\mathbf{g}j}$ implies $j \equiv 1 \bmod p^m$ and therefore $\mathbf{g} = \mathbf{g}'$.

(11.7) *If G is a direct product of a cyclic group of order p^n $(0 < n)$ and of a group of type p^∞, and if G and the group H are subgroup-isomorphic, then G and H are (element-)isomorphic.*

Proof. If f is a subgroup-isomorphism of G upon the group H, then it follows from Corollary 11.3 that f is index-preserving. G contains exactly one subgroup T of type p^∞, and consequently T^f is a normal subgroup of H and of type p^∞ (cp. Corollary 4.4). Denote by G' the subgroup of all the elements of an order dividing p^n. Then G/G' is of type p^∞. $G'^f = H'$ is the subgroup of all the elements of H whose order divides p^n (by (2.2)!) and is therefore a normal subgroup of H. As H' contains but a finite number of subgroups, H' is a finite group and the group of the automorphisms of H' is finite. Let p^m be the highest power of p so that there exist automorphisms of order p^m of H'. If x is any element in $T' = T^f$, then T' contains an element y so that $y^{p^m} = x$. As the order of y is a power of p, the order of the automorphism which y induces in the normal subgroup H' of H is a power of p and $x = y^{p^m}$ consequently induces the identical automorphism in H'. Thus every element in T' is permutable with every element in H'.—If G is the direct product of T and the cyclic group Z of order p^n, then $Z \leq G'$, $Z^f \leq H'$ and H is consequently the direct product of Z^f and T'. Since f is index-preserving, this shows that G and H are isomorphic groups.

If G is a group, i a not-negative integer, then denote by $(G; x^i = 1)$ the subgroup of G which is generated by those elements x in G which satisfy $x^i = 1$. If G is an abelian group, then every element in $(G; x^i = 1)$ satisfies $x^i = 1$.

Suppose now that G is an abelian p-group, but not ideal-cyclic. Then it may happen that $(G; x^p = 1)$ contains less than p^3 elements. Then $(G; x^p = 1)$ is the direct product of two cyclic groups of order p and we put $m = m(G) = 0$. A second possibility is that there exists a greatest positive integer $m = m(G)$ so that $(G; x^{p^m} = 1)/(G; x^{p^{m-1}} = 1)$ contains at least p^3 elements and $(G; x^{p^{m+1}} = 1)/(G; x^{p^m} = 1)$ contains at most p^2 elements. Then $G/(G; x^{p^m} = 1)$ is a direct product of two ideal-cyclic groups one or both of which may be equal 1. Finally it may happen that for every integer i the quotient group $(G; x^{p^{i+1}} = 1)/(G; x^{p^i} = 1)$ contains at least p^3 elements. Then we put $m = m(G) = \infty$.

THEOREM 11.8. *Suppose that G is an abelian p-group which is not ideal-cyclic and that f is a subgroup-isomorphism of G upon the group H.*

(a) *f is induced by an (element-)isomorphism of G, if one of the following conditions is satisfied:*

(a. 1) *G contains at least p^3 elements, $G^p = 1$ and f is index-preserving.*

(a. 2) $1 < m(G) < \infty$ *and* $G = (G; x^{p^{m(G)}} = 1)$.

(a. 3) $m(G) = \infty$.

(b) *If the orders of the elements in G are not bounded, then G and H are (element-)isomorphic.*

(c) *If H is abelian, then there exists an (element-)isomorphism of G upon H which induces f in $(G; x^{p^{m(G)}} = 1)$ (if $m(G)$ is finite).*

Proof. It is a consequence of Theorem 11. 2 and of the Corollaries 11. 3 and 11. 4 that *f is index-preserving,* if either of the conditions mentioned in the Theorem 11. 8 is satisfied. Hence it follows from Lemma 11. 5, that f is induced by an isomorphism of G upon H, if either (a. 1) or (a. 2) is satisfied.

Assume now that (a. 3) is satisfied. If i is any positive integer, then there exists by Lemma 11. 5 an isomorphism g of $(G; x^{p^i} = 1)$ upon $(G; x^{p^i} = 1)^f$ which induces f in $(G; x^{p^i} = 1)$. Furthermore there exists an element w of order p^{i+1} in G so that $u = w^p$ is an element of the exact order p^i. Since $\{u\}^f \leq \{w\}^f$, it follows that there exists an element w' so that $\{w\}^f = \{w'\}$ and $u^g = w'^p$. There exists by Corollary 11. 6 an isomorphism h of $(G; x^{p^{i+1}} = 1)$ which induces f and maps w upon w'. Then we have $u^g = w'^p = w^{hp} = w^{ph} = u^h$. Since h induces f in $(G; x^{p^i} = 1)$ and maps u upon the same element as g, it follows from Corollary 11. 6 that g and h coincide in $(G; x^{p^i} = 1)$.—This proves that there exists to every positive integer i an isomorphism $g(i)$ of $(G; x^{p^i} = 1)$ which induces f and coincides with $g(j)$ in $(G; x^{p^j} = 1)$ for $j < i$. Since G is the join of all the groups $(G; x^{p^i} = 1)$, there exists one and only one isomorphism g of G which coincides in every $(G; x^{p^i} = 1)$ with $g(i)$. This isomorphism g induces f in every cyclic subgroup of G and therefore g induces f everywhere.

Thus (a) is completely proved. If the orders of the elements in G are not bounded, then either $m(G) = \infty$ and it follows from (a) that f is induced by an isomorphism of G. If on the other hand $m(G)$ is finite, then $G/(G; x^{p^{m(G)}} = 1)$ is a direct product of two ideal-cyclic groups and one of them is of type p^∞, as the orders of the elements in G are not bounded. Hence G contains a group of type p^∞ and is therefore [13] the direct product of a group

[13] Cp. e. g. R. Baer,[11], section 1.

G' and of a group T of type p^∞. It is a consequence of (11.7) that T^f is contained in the central of H and it is therefore a consequence of (9.6) that G'^f and therefore that H is abelian. Thus (b) will be proved as soon as (c) has been proved.

Assume now that H is abelian, that $m(G)$ is finite and that $(G; x^{p^{m(G)}} = 1) \neq G$—if these latter assumptions would not be satisfied then (c) would be a consequence of (a). $G/(G; x^{p^{m(G)}} = 1)$ is a direct product of one or two ideal-cyclic groups and consequently there exist elements $a(i)$, $b(i)$ for $i = 0, \cdots$ which generate G mod $(G; x^{p^{m(G)}} = 1)$ so that $a(i), b(i)$ are both of the exact order $p^{i+m(G)}$ and are independent, if $\neq 1$—it may happen that $b(i)$ is only defined for $i = 0$ and that both are defined only for a finite number of i's—and so that finally $a(i+1)^p = a(i)$, $b(i+1)^p = b(i)$. There exists by Lemma 11.5 an isomorphism $\boldsymbol{h}$ of $(G; x^{p^{m(G)}} = 1)$ which induces $\boldsymbol{f}$ in $(G; x^{p^{m(G)}} = 1)$. Since H is abelian and $\boldsymbol{f}$ is index-preserving, there exist elements $a(i)'$, $b(i)'$ so that $\{a(i)\}^f = \{a(i)'\}$, $\{b(i)\}^f = \{b(i)'\}$, $a(0)^h = a(0)'$, $b(0)^h = b(0)'$, $a(i+1)'^p = a(i)'$, $b(i+1)'^p = b(i)'$.

There exists exactly one isomorphism $\boldsymbol{g}$ of G which coincides with $\boldsymbol{h}$ in $(G; x^{p^{m(G)}} = 1)$, maps $a(i)$ upon $a(i)'$ and $b(i)$ upon $b(i)'$. Since the $a(i)$ and $b(i)$ generate G mod $(G; x^{p^{m(G)}} = 1)$, it follows that $\boldsymbol{g}$ maps G upon the whole group H and this completes the proof.

Remarks. That there exist index-preserving subgroup-isomorphisms of abelian finite p-groups upon non-abelian groups, has been shown by Rottländer.[14] Thus it is impossible to omit in (c) the hypothesis that H is abelian.

That there exist subgroup-automorphisms which are not induced by element-automorphisms has been noted before. Thus it is impossible to strengthen the statement in (c) in such a way that it becomes analogous to (a). The following statement may be of some interest in this connection:[15]

Let G be a direct product of cyclic groups of order p. Then there exist subgroup-automorphisms of G which are not induced by element-automorphisms if, and only if,

G is of order p^2 and $p \neq 2$ and $\neq 3$.

If the order of G is p, then G is cyclic and the identity is the only subgroup-automorphism. If the order of G is greater than p^2, then it is a consequence

[14] Rottlaender [1].

[15] This statement and Theorem 11.8 contradict Theorem 5.1 in the author's paper [11]. But the "proof" of this assertion was based on the erroneous assumption that subgroup-automorphisms of direct factors are induced by subgroup-automorphisms of the product.

of Theorem 11. 8, (a) and of Corollary 11. 4 that every subgroup-isomorphism of G is induced by an element-automorphism of G. If finally G is of order p^2, then the order of its group of automorphisms is $(p^2-1)p(p-1)$ and the number of subgroup-automorphisms which are induced by element-automorphisms is therefore $(p-1)p(p+1)$ as the element-automorphism g of G induces the identical subgroup-automorphism[16] if, and only if, $x^g = x^j$ for every x in G where j is independent of x and $0 < j < p$. The number of the subgroup-automorphisms of G is exactly $(p+1)!$ since the subgroup-automorphisms are exactly the permutations of the $p+1$ proper subgroups of G. But $(p+1)! = (p-1)p(p+1)$ if and only if $p=2$ or $p=3$ and this completes the proof of our statement.

12. Abelian groups with elements of infinite order. If G is an abelian group, then the elements of finite order in G form a subgroup $F(G)$ of G which consists of elements of finite order only, and $G/F(G)$ does not contain elements $\neq 1$ of finite order. Throughout this and the following section we shall assume that G contains elements of infinite order ($G \neq F(G)$) and the greater part of this section will be devoted to those groups G where $G/F(G)$ is $\neq 1$ and ideal-cyclic, since the groups which contain two independent elements of infinite order will be investigated in the next section.

The p-component of $F(G)$ may be denoted by $F(G,p)$. Then $(G; x^{p^i}=1) = (F(G,p); x^{p^i}=1)$ for every integer i. The number $m(G,p)$ shall be defined as follows:

$$m(G,p) = \begin{cases} 0, \text{ if } (G; x^p = 1) \text{ is a cyclic group;} \\ i, \text{ if } (G; x^{p^{i+1}}=1)/(G; x^{p^i}=1) \text{ is cyclic, but} \\ \qquad (G; x^{p^i}=1)/(G; x^{p^{i-1}}=1) \text{ is not cyclic;} \\ \infty, \text{ if } (G; x^{p^{i+1}}=1)/(G; x^{p^i}=1) \text{ is never cyclic.} \end{cases}$$

Then the join-group $M(G)$ of all the subgroups $(G; x^{p^i}=1)$ for $i \leq m(G,p)$ is a smallest subgroup of G so that $F(G)/M(G)$ is ideal-cyclic.—If $m(G,p)$ is finite, then $F(G,p)/(G; x^{p^{m(G,p)}}=1)$ is either a finite cyclic group or a group of type p^∞. Therefore[17] both $F(G)$ and $F(G,p)$ are direct products of an ideal-cyclic group and of a subgroup of $M(G)$.—Finally it may be recalled that the prime number p is relevant for G, if $F(G,p) \neq 1$, and otherwise p is irrelevant.

LEMMA 12. 1. *If the abelian group G contains elements of infinite order and if f is a subgroup-isomorphism of G upon the group H, then*

(a) $F(G)^f = F(H)$ *is the subgroup of all the elements of finite order in H;*

[16] Cp. [11].

[17] Cp. Baer,[11] section 1.

(b) *there exists an isomorphism of* $F(G)$ *upon* $F(H)$ *which induces* f *in (the set of subgroups of)* $M(G)$;

(c) $Z^{pf} = Z^{fp}$ *for every cyclic subgroup* Z *of* G *and for every for* G *relevant prime number* p (or as we shall say: f *preserves the relevant indices*);

(d) *there exists to every prime number* p *and to every element* t *of infinite order in* H *an integral* p*-adic number* $j(p,t)$ *so that*

$$txt^{-1} = x^{1+pj(p,t)} \text{ for } x \text{ in } F(H,p)$$

and so that $j(p,t) = 0 \bmod p^i$, *if* t *is mod* $F(H)$ *a* p^i*-th power.*

Remark. If $G/F(G) = (G/F(G))^p$, *then* $F(H,p)$ *is contained in the central of* H, since either $F(G,p) = F(H,p) = 1$ (by our Lemma) or $H/F(H) = (H/F(H))^p$ (by our Lemma), and since therefore every element t of infinite order in H is mod $F(H)$ a p^i-th power for every i and this implies $j(p,t) = 0$ by (d) of the Lemma.

Proof. It is a consequence of the Theorems 2. 4 and 3. 2 that subgroup-isomorphisms map finite cyclic groups upon finite cyclic groups and infinite cyclic groups upon infinite cyclic groups. Hence $F(G)^f$ is exactly the set of all the elements of finite order in H and this proves (a).

A particular consequence of this fact is the following one: If x is an element of finite order in H and y is an element of infinite order in H, then $\{x\} = F(\{x,y\})$. Thus $\{x\}$ is a normal subgroup of $\{x,y\}$ and yxy^{-1} is a power of x.

If now x and y are two elements of finite order in H, then $\{x,y\}$ is generated by two independent elements u and v—unless it is a cyclic group. If t is some element of infinite order in H, then it follows from what has just been proved that

$$\begin{aligned} tuvu^{-1}v^{-1}t^{-1} &= tut^{-1}(tv)u^{-1}(tv)^{-1} = u^h \\ &= (tu)v(tu)^{-1}tv^{-1}t^{-1} = v^k \end{aligned}$$

for suitable integers h and k, since t, tu and tv are elements of infinite order in H. Since u and v are independent this implies $t\,uvu^{-1}v^{-1}t^{-1} = 1$. Consequently $uv = vu$ so that we have proved:

(12. 1. 1) $F(H)$ *is abelian.*

If x is an element of the finite order n in H, t an element of infinite order in H, then $\{x\}^{f^{-1}}$ is a finite cyclic group $\{x'\}$ of some order m and $\{t\}^{f^{-1}}$ is an infinite cyclic group $\{t'\}$. As G is abelian, $\{x', t'\}$ is the direct product of $\{x'\}$ and $\{t'\}$. Since $\{t'^{m^2}\}$ is the only infinite cyclic subgroup of $\{x', t'\}$ so that $\{x', t'\}/\{t'^{m^2}\}$ is a direct product of a cyclic group of order m and of a cyclic

group of order m^2, it follows that $\{t'^{m^2}\}^f$ is a normal subgroup of $\{x', t'\}^f = \{x, t\}$. It is now a consequence of Corollary 11.3 that f is index-preserving on $\{x', t'\}/\{t'^{m^2}\}$. This implies in particular that both x and x' are of order $n = m$ and that $\{t'^{n^2}\}^f = \{t^{n^2}\}$ and this fact is equivalent to (c).

If t is an element of infinite order in H, then it is a consequence of facts which have been proved in the second paragraph of this proof that t induces in $F(H)$ and in $F(H, p)$ an automorphism which maps every subgroup of $F(H)$ into itself. Thus it follows from well known facts [11] that there exists an integral p-adic number $i(p, t)$ so that $txt^{-1} = x^{i(p,t)}$ for every x in $F(H, p)$. If x' and t' are elements in G, so that $\{x'\}^f = \{x\}$ and $\{t'\}^f = \{t\}$, then $\{x', t'\}$ is the direct product of $\{x'\}$ and $\{t'\}$. Since $\{x'^p, t'^p\}$ is the only subgroup of $\{x', t'\}$ so that $\{x', t'\}/\{x'^p, t'^p\}$ is a direct product of two cyclic groups of order p, it follows that $\{x'^p, t'^p\}^f$ is a normal subgroup of $\{x, t\} = \{x', t'\}^f$ and f consequently induces (by (c)!) an index-preserving subgroup-isomorphism of $\{x', t'\}/\{x'^p, t'^p\}$ upon $\{x, t\}/\{x, t\}^p$. Hence it follows from Theorem 8.1 that $\{x, t\}/\{x, t\}^p$ is abelian and $txt^{-1}x^{-1}$ is therefore a p-th power, i. e. $i(p, t) - 1 = pj(p, t)$. Since $t^pxt^{-p} = x^{i(p,t)^p}$ it follows that $j(p, t^p) \equiv 0 \bmod p$ and this completes the proof of (d).

Let now u be an element of infinite order in G and u' an element in H so that $\{u\}^f = \{u'\}$. Then it follows from (9.2) and (d) that there exists for every element x in $F(G)$ one and only one element $x' = f(x; u, u', f)$ in $F(H)$ so that

$$\{x\}^f = \{x'\}, \qquad \{xu\}^f = \{x'u'\}.$$

It is a consequence of (9.4) and (9.5) that $f(x; u, u', f)$ is an isomorphism of $M(G)$ upon $M(G)^f$ which induces f in the sets of subgroups of $M(G)$.

Since $F(G)/M(G)$ is ideal-cyclic, since either the orders of the elements in $F(G)/M(G)$ are prime to p or the orders of the elements in the p-component of $M(G)$ are bounded, there exist elements $a(p, i)$ in $F(G, p)$ which generate $F(G)$ mod $M(G)$ and satisfy: $a(p, i + 1)^p = a(p, i)$ and $a(p, 0) \equiv 1 \bmod M(G)$.

$F(H)$ is an abelian group by (12.1.1) and f is by (c) index-preserving on $F(G)$. Consequently there exist elements $a(p, i)^*$ in $F(H)$ so that

$$a(p,0)^* = f(a(p,0); u, u', f), \ \{a(p,i)\}^f = \{a(p,i)^*\}, \ a(p,i+1)^{*p} = a(p,i)^*.$$

There exists one and only one isomorphism g of $F(G)$ which coincides with $f(x; u, u', f)$ on $M(G)$ and maps $a(p, i)$ upon $a(p, i)^*$; g maps $F(G)$ upon the whole group $F(H)$ since the elements $a(p, i)^*$ generate $F(H)$ mod $M(G)^f$. Thus (b) holds true and this completes the proof of the Lemma.—The isomorphism g which has just now been constructed has a certain property which may be stated for future reference.

COROLLARY 12. 2. *If u is an element of infinite order in the abelian group G, if f is a subgroup-isomorphism of G upon the group H and if $\{u\}^f = \{u'\}$, then there exists an isomorphism g of $F(G)$ upon $F(H)$ so that $\{x\}^f = \{x^g\}$, $\{xu\}^f = \{x^g u'\}$ for x in $M(G)$.*

THEOREM 12. 3. *If G is an abelian group so that $G/F(G)$ is an ideal-cyclic group $\neq 1$ and if there exists an index-preserving subgroup-isomorphism between G and the abelian group H, then G and H are isomorphic.*

Proof. It is known [18] that G is a direct product of a group G' without subgroups of type p^∞ and of a group $G'' \leq F(G)$ which satisfies $G'' = G''^n$ for every positive integer n. Then $G/F(G)$ and $G'/F(G')$ are essentially the same groups.

Let now b be any element of infinite order in G'. Then we put:

$$n(p) = \begin{cases} \infty, & \text{if } F(G')b \text{ is contained in every } (G'/F(G'))^{p^i}; \\ i, & \text{if } F(G')b \text{ is contained in } (G'/F(G'))^{p^i}, \text{ but not in} \\ & \qquad (G'/F(G'))^{p^{i+1}}. \end{cases}$$

(12. 3. 1) If $n(p) = \infty$, but the orders of the elements in $F(G', p)$ are bounded, then there exist elements $b(p, i)$ so that $b(p, 1)^p b^{-1} = w(p)$ is an element in $F(G', p)$ and $b(p, i)^p = b(p, i-1)$ for $0 < i$.

If $n(p) = \infty$, then there exist elements $c(p, i)$ so that $c(p, 0) = b$. The element $c(p, i)^p c(p, i-1)^{-1} = v(i)$ lies in $F(G', p)$, since G' is abelian and since an equation $x^p = u$ has a uniquely determined solution in $\{u\}$, if u is an element $\neq 1$ of finite order whose order is prime to p. Since we assumed that the orders of the elements in $F(G', p)$ are bounded, there exists a positive integer k so that $x^{p^k} = 1$ for every x in $F(G', p)$.

From the definition of the elements $c(p, i)$ and $v(i)$ it follows by complete induction that

$$(12.3.11) \qquad c(p, i+s)^{p^s} = c(p, i) \prod_{h=0}^{s-1} v(i+1+h)^{p^h}.$$

Now the elements $b(p, i)$ may be defined as follows for $0 < i$:

$$b(p, jk - i) = c(p, (j+1)k)^{p^{i+k}} \text{ for } 0 < j \text{ and } 0 \leq i < k.$$

Applying (12. 3. 11) and $x^{p^k} = 1$ for x in $F(G', p)$ it follows that

$$b(p, jk - i) = c(p, jk - i + i + k)^{p^{i+k}} = c(p, jk - i) \prod_{h=1}^{i+k} v(jk - i + h)^{p^{h-1}}$$
$$= c(p, jk - i) \prod_{h=1}^{k} v(jk - i + h)^{p^{h-1}}$$

---

[18] Reinhold Baer, "The subgroup of the elements of finite order of an abelian group," *Annals of Mathematics*, vol. 37 (1936), pp. 766-781, (1; 1).

so that in particular $b(p, jk-i)c(pjk-i)^{-1}$ is in $F(G', p)$. Furthermore we have

$$\begin{aligned} b(p, jk-i)^p &= c(p, jk-i)^p \prod_{h=1}^{k} v(jk-i+h)^{p^h} \\ &= c(p, jk-i-1)v(jk-i) \prod_{h=1}^{k-1} v(jk-i+h)^{p^h} \\ &= b(p, jk-i-1), \text{ if } jk-i-1 \neq 0 \text{ and} \\ &= b\prod_{h=0}^{k-1} v(1+h)^{p^h} = bw(p) \quad \text{for} \quad jk-i-1=0 \end{aligned}$$

and this completes the proof of (12.3.1).

(12.3.2) If $n(p)$ is finite, then there exists an element $b(p)$ so that $b(p)^{p^{n(p)}}b^{-1} = w(p)$ is an element in $F(G', p)$.

(12.3.3) If $n(p)$ is infinite and the orders of the elements in $F(G', p)$ are not bounded, then there exist elements $b(p, i)$ for $0 \leq i$ so that $b = b(p, 0)$ and $b(p, i+1)^p\, b(p, i)^{-1} = w(p, i)$ is an element of $F(G', p)$.

Both (12.3.2) and (12.3.3) are obvious consequences of the facts that G' is abelian and that an equation $x^n = u$ has exactly one solution in $\{u\}$, if n and the finite order of u are relatively prime.

If the elements $b(p)$ for finite $n(p)$ and $b(q, i)$ for infinite $n(q)$ are determined in accordance with (12.3.1) to (12.3.3), then these elements generate G' mod $F(G')$ and they generate G mod $F(G)$.

Since H is abelian, H is the direct product of its subgroups $H' = G'^f$ and $H'' = G''^f$. It is furthermore a consequence of our hypothesis concerning f and of Lemma 12.1 that f is index-preserving.

Let now c be an element in H so that $\{b\}^f = \{c\}$. Then it is a consequence of Corollary 12.2 and of the proof of Lemma 12.1 that there exists an isomorphism g of $F(G)$ upon $F(H)$ with the following properties:

(i) $\{x\}^f = \{x^g\}$, $\{xb\}^f = \{x^g c\}$ for x in $M(G)$.

(ii) $G''^g = H''$ (as G'' is the greatest subgroup of $F(G)$ which satisfies: $G'' = G''^n$ for every positive n).

(iii) $F(H') = F(G')^g$.

It is a consequence of (9.2) and the fact that H is abelian that there exists to every element x in $F(G)$ one and only one element $x' = f(x; b, c, f)$ so that

$$\{x\}^f = \{x'\} \text{ and } \{xb\}^f = \{x'c\}.$$

It follows from (i) that

$$x^g = f(x; b, c, f) \text{ for } x \text{ in } M(G).$$

If u is an element of infinite order in G, p a prime number and v an element so that $\{v\} = \{u^p\}^{\boldsymbol{f}}$, then there exists one and only one element v' so that $\{v'\} = \{u\}^{\boldsymbol{f}}$ and $v'^p = v$, since $\boldsymbol{f}$ is index-preserving. Consequently there exist elements $c(p)$ for finite $n(p)$ and $c(q, i)$ for infinite $n(q)$ with the following properties:

(I) If $n(p)$ is finite, then $\{b(p)\}^{\boldsymbol{f}} = \{c(p)\}$ and $c(p)^{p^{n(p)}} = cf(w(p); b, c, \boldsymbol{f})$.

(II) *If* $n(p)$ is infinite, but the orders of the elements in $F(G', p)$ are bounded, then $\{b(p, i)\}^{\boldsymbol{f}} = \{(c(p, i)\}$ and $c(p, i+1)^p = c(p, i)$, $c(p, 1)^p = cf(w(p); b, c, \boldsymbol{f})$.

(III) If $n(p)$ is infinite and the orders of the elements in $F(G', p)$ are not bounded, then $\{b(p, i)\}^{\boldsymbol{f}} = \{c(p, i)\}$ and $c(p, i+1)^p = c(p, i) f(w(p, i); b, c, \boldsymbol{f})$ for $0 \leq i$.

If p is a prime number so that $F(G', p)$ is not contained in $M(G)$, then $F(G', p) = F(G, p)$ is the direct product of a cyclic group $\{z(p)\}$ of order $p^{h(p)}$ with $m(G, p) < h(p)$ and of a group $M'(G, p)$ which is contained in $M(G)$. Then an element $w(p)$ is defined according to (12.3.1) and (12.3.2) and $w(p)$ has the form: $w(p) = v(p) z(p)^{k(p)}$ for $v(p)$ in $M'(G, p)$.

Since

$$z(p)^{\boldsymbol{g} p^{h(p)-m(G,p)}} = z(p)^{p^{h(p)-m(G,p)} \boldsymbol{g}} = f(z(p)^{p^{h(p)-m(G,p)}}; b, c, \boldsymbol{f}),$$

it follows that there exists an element $z(p)'$ in $M'(G, p)$ so that $f(z(p); b, c, \boldsymbol{f})$ and $(z(p) z(p)')^{\boldsymbol{g}}$ generate the same subgroup. There exists therefore an integer $j(p)$ prime to p so that

$$f(z(p)^{k(p)}; b, c, \boldsymbol{f}) = (z(p)^{k(p)} z(p)^{k(p)})^{\boldsymbol{g} j(p)}.$$

Thus there exists an isomorphism $\boldsymbol{r}$ of $F(G)$ upon $F(H)$ with the following properties which determine $\boldsymbol{r}$ uniquely:

$x^{\boldsymbol{r}} = x^{\boldsymbol{g}}$, if x is an element in G'' or in an $F(G', p)$ which is contained in $M(G)$ or in $M'(G, p)$ in case $F(G', p)$ is not part of $M(G)$;

$z(p)^{\boldsymbol{r}} = (z(p) z(p)')^{\boldsymbol{g} j(p)}$ if $F(G', p)$ is not contained in $M(G)$.

This isomorphism $\boldsymbol{r}$ satisfies in particular:

$$w(p)^{\boldsymbol{r}} = f(w(p); b, c, \boldsymbol{f}), \qquad w(p, i)^{\boldsymbol{r}} = f(w(p, i); b, c, \boldsymbol{f}).$$

For if $w(p, i)$ is defined, then $F(G', p) \leq M(G)$ and $x^{\boldsymbol{r}} = x^{\boldsymbol{g}} = f(x; b, c, \boldsymbol{f})$ for elements x in $F(G', p)$. The same applies to $w(p)$ such that $F(G', p) \leq M(G)$. If $w(p)$ is defined, but $F(G', p)$ is not part of $M(G)$, then

$$\begin{aligned} f(w(p)\,;b,c,\mathfrak{f}) &= f(v(p)\,;b,c,\mathfrak{f})f(z(p)^{k(p)}\,;b,c,\mathfrak{f}) \text{ by } (9.4) \\ &= v(p)^{g}(z(p)^{k(p)}z(p)'^{k(p)})^{gj(p)} \\ &\qquad\qquad \text{as } v(p) \text{ is in } M(G,p)', \\ &= v(p)^{\mathfrak{r}}z(p)^{\mathfrak{r}} = w(p)^{\mathfrak{r}}. \end{aligned}$$

In mapping $b(p)$ upon $c(p)$, $b(p,i)$ upon $c(p,i)$ and b upon c an extension of the isomorphism $\mathfrak{r}$ to an isomorphism of G upon H may be defined as follows from (I) to (III). This completes the proof of our theorem. As a matter of fact we have proved slightly more, namely:

Corollary 12. 4. *If G is an abelian group so that $G/F(G)$ is an ideal-cyclic group $\neq 1$, and if $\mathfrak{f}$ is a subgroup-isomorphism of G upon the group H (which preserves the for G irrelevant indices), then there exists an isomorphism $\mathfrak{r}$ of G upon H and a subgroup R of $F(G)$ with the following properties:*

(i) *$\mathfrak{r}$ induces $\mathfrak{f}$ in the set of subgroups of R;*

(ii) *$F(G)/R$ is ideal-cyclic and the p-components of $F(G)/R$ are finite;*

(iii) *$F(G,p) \leq R$, if either $F(G,p) \leq M(G)$ or if $F(G,p)$ contains a subgroup of type p^∞.*

Corollary 12. 5. *If G is an abelian group so that $G/F(G)$ is an ideal-cyclic group $\neq 1$, and if $\mathfrak{f}$ is a subgroup-isomorphism of G upon the abelian group H, then $G/F(G)$ and $H/F(H)$ are subgroup-isomorphic and there exists an isomorphism of $F(G)$ upon $F(H)$, inducing $\mathfrak{f}$ in the set of subgroups of $M(G)$.*

The two most important special cases of these statements may be enunciated separtely:

If G is an abelian group so that $G/F(G)$ is an ideal-cyclic group $\neq 1$, and if there exists an index-preserving subgroup-isomorphism between G and the abelian group H, then G and H are (element-)isomorphic.

If G is an abelian group so that $G/F(G)$ is an ideal-cyclic group $\neq 1$, and so that either $F(G,p) \leq M(G)$ or the orders of the elements in $F(G,p)$ are not bounded, and if $\mathfrak{f}$ is a subgroup-isomorphism of G upon the abelian group H which preserves the for G irrelevant indices, then there exists an isomorphism $\mathfrak{r}$ of G upon H which induces $\mathfrak{f}$ in the set of subgroups of $F(G)$.

Remarks. That the condition concerning the preservation of indices cannot be omitted, is a consequence of the fact that there exist subgroup-automorphisms of ideal-cyclic groups without elements $\neq 1$ of finite order which are not index-preserving (cp. sections 3 and 4).

The following *example* shows that it is impossible to strengthen our

statements concerning the induction of the given subgroup-isomorphism by some element-isomorphism.

Let p be a prime number $\neq 2$ and G a direct product of some cyclic groups of order p and of an infinite cyclic group $\{z\}$. Then a subgroup-automorphism f of G may be defined as follows:

If t is an element of finite order, k is prime to p and h a not negative integer, then

$$\{t\}^f = \{t\}, \qquad \{tz^{kp^h}\}^f = \{t^{(-1)^h} z^{kp^h}\}.$$

That such a subgroup-automorphism exists, is a consequence of the fact that p-th powers $\neq 1$ in G are powers of the element z. On the other hand it is clear that f is not induced by any automorphism of G.

Finally we construct an *example of an abelian group G which contains elements of infinite order and possesses an index-preserving subgroup-isomorphism upon a not-abelian group.*

Let G be a direct product of a cyclic group of order p^2 (p a prime number $\neq 2$) and of an infinite cyclic group and let H be the group which is generated by two elements u, v which obey the following rules:

$$u^{p^2} = 1, \qquad vuv^{-1} = u^{1+p}.$$

Then every element of H has the form $u^i v^j$ where i and j are integers, $0 \leq i < p^2$, and where i and j are uniquely determined by the element. If i, j, and $0 < k$ are integers, then

$$v^j u^i v^{-j} = u^{i(1+jp)}, \qquad (u^i v^j)^{-1} = u^{-i(1-jp)} v^{-j},$$
$$(u^i v^j)^k = u^{i(k+jpk(k-1)2^{-1})} v^{kj}.$$

These formulae imply that the central of H is the direct product of $\{u^p\}$ and $\{v^p\}$ and that the central quotient group of H is a direct product of two cyclic groups of order p.

If a, b is a basis of G so that b is an element of infinite order, then a subgroup-isomorphism of G upon H which preserves indices may be defined by mapping

$\{a^{ik} b^k\}$ upon $\{u^{i(k+pk(k-1)2^{-1})} v^k\}$ for positive k prime to p

$\{a^i b^{pk}\}$ upon $\{u^i v^{pk}\}$

and non-cyclic subgroups may be mapped accordingly, since the non-cyclic subgroups of H always contain $\{u^p\}$.

13. Abelian groups which contain at least two independent elements of infinite order.

THEOREM 13. 1. *If the abelian group G contains at least two independent*

elements of infinite order, then every subgroup-isomorphism of G is induced by an (element-)isomorphism of G.

Proof. If f is some subgroup-isomorphism of the group G upon the group H, then it is a consequence of Lemma 12.1 that $F(G)^f$ is the subgroup $F(H)$ of all the elements of finite order in H, that $F(G)$ and $F(H)$ are isomorphic and that therefore $F(H)$ is abelian.

If x and y are any two elements in H, then let V be the subgroup of G so that $V^f = \{x, y\}$. V is generated by two elements and therefore either cyclic or a direct product of two cyclic groups. If V is cyclic, then so is V^f and x and y are permutable elements. If V is finite, then $V \leq F(G)$ and both x and y are elements in the abelian group $F(H)$ and x and y are permutable.—Assume now that V is a direct product of two infinite cyclic groups. Since V is abelian, it follows from Corollary 11.4 and Corollary 8.2 that V^p is the only subgroup S of V so that V/S is subgroup-isomorphic to a direct product of two cyclic groups of the prime number order p. Since conjugate subgroups of $\{x, y\}$ possess isomorphic lattices of containing subgroups, this implies that V^{pf} is a normal subgroup of $\{x, y\}$. Thus f induces a subgroup-isomorphism of V/V^p upon $\{x, y\}/V^{pf}$. Lemma 5.1 proves now that the direct product V/V^2 of two cyclic groups of order 2 and $\{x, y\}/V^{2f}$ are isomorphic. Therefore f preserves the index 2, and the commutator group of $\{x, y\}$ is contained in V^{2f}. Assume now—by induction—that for every prime number $q < p$ the direct product V/V^q of two cyclic groups of order q and $\{x, y\}/V^{qf}$ are isomorphic groups so that in particular f preserves—in V—the index q for every prime number $q < p$. The subgroup-isomorphism f of V/V^p therefore maps cyclic groups of order p upon cyclic groups whose order is not smaller than p. But this implies by Theorem 8.1 that V/V^p and $\{x, y\}/V^{pf}$ are isomorphic; hence we have proved by complete induction that

V/V^p and $\{x, y\}/V^{pf}$ are isomorphic groups for every prime number p and f is index-preserving on V.

The commutator group of $\{x, y\}$ is consequently contained in the meet of all the groups V^{pf}. This implies that $\{x, y\}$ is abelian since the meet of all the groups V^p is equal to 1.

Thus x and y are permutable elements, if V is a direct product of two infinite cyclic groups.—If finally V is a direct product of a finite cyclic group $\{u\}$ and an infinite cyclic group $\{v\}$, then there exists in G an element w of infinite order which is independent of v. It follows from the fact which has been proved just now that both $\{v, w\}^f$ and $\{v, uw\}^f$ are abelian groups. Thus $\{v\}^f$ is part of the central of $\{v, w, uw\}^f = \{v, w, u\}^f$ and $\{v\}^f$ is therefore part of the central of $\{v, u\}^f = \{x, y\}$. Thus the central quotient group of $\{x, y\}$ is cyclic. This proves that $\{x, y\}$ is abelian and that x and y are in any case permutable elements. Hence

H is abelian.

It is a consequence of Lemma 12. 1 that f preserves the indices of finite cyclic subgroups. If Z is an infinite cyclic subgroup, then Z is a direct factor of a direct product V of two infinite cyclic groups, $V \leq G$. But it has just been proved that f is index-preserving on such subgroups V. Thus it follows that

f is index-preserving.

Let u be an element of infinite order in G and u' an element in H so that $\{u\}^f = \{u'\}$. Then there exists by (9. 2) to every element x in G which is independent of u one and only one element $x' = f(x; u, u', f)$ so that

$$\{x\}^f = \{x'\}, \qquad \{xu\}^f = \{x'u'\}.$$

As a consequence of (9. 4) and (9. 5) this function $f(\ldots)$ *is an isomorphism of $F(G)$ upon $F(H)$*. Furthermore

$$f(xy; u, u', f) = f(x; u, u', f)f(y; u, u', f)$$

if the following conditions are satisfied: x and y are both independent of u; and they are independent of each other, if they are both of infinite order.

If x and u are dependent elements, then x is of infinite order and the meet of $\{x\}$ and $\{u\}$ is $\{u^d\}$ for some positive number d. Then $x^i = u^d$ for some uniquely determined integer i. Moreover, there exists one and only one element $x' = f(x; u, u', f)$ so that

$$\{x\}^f = \{x'\}, \qquad x'^i = u'^d,$$

since f is index-preserving and $|i|$ is the index of the meet of $\{u\}$ and $\{x\}$ in $\{x\}$.

Thus $f(x; u, u', f)$ is a single valued function which is defined for every x in G, every element u of infinite order in G and every u' so that $\{u\}^f = \{u'\}$. Some simple properties of this function may be mentioned.

(13. 1. 1) $\{x\}^f = \{f(x; u, u', f)\}$.

(13. 1. 2) If u and v are independent elements of infinite order, and if $v' = f(v; u, u', f)$, then $u' = f(u; v, v', f)$.

(13. 1. 3) $f(x; u^{-1}, u', f) = f(x; u, u'^{-1}, f) = f(x; u, u', f)^{-1}$.

The proof of the following statement constitutes the basic step for the proof of our theorem.

(13. 1. 4) If u and v are independent elements of infinite order, then $f(x; u, u', f)$ is an isomorphism of $\{u, v\}$ which induces f in the set of subgroups of $\{u, v\}$.

Put $v' = f(v; u, u', f)$. Then $\{u^i\}^f = \{u'^i\}$ and $\{v^j\}^f = \{v'^j\}$, since f is index-preserving. Hence it follows from (9.1) that $\{u^i v^j\}^f$ is generated by an element of the form $u'^i v'^{je(i,j)}$ where $e(i,j) = \pm 1$ and where $e(i, -j) = e(i,j)$ and $e(i,j) = e(-i, -j)$ for $i \neq 0$. Since $e(i,j)$ is only uniquely determined by the above conditions, if both i and j are $\neq 0$, we put $e(i, 0) = e(0, j) = 1$. If both i and j are $\neq 0$, then the above identities for $e(i,j)$ permit us to assume that both i and j are positive. Then u and $u^{i-1}v$ are independent and it follows from (9.1) that $\{u^i v^j\}^f = \{u(u^{i-1}v^j)\}^f$ is generated by an element of the form $u'(u'^{i-1}v'^{je(i-1,j)})^d$ with $d = \pm 1$. Since u' and v' are independent elements of infinite order, this implies:

$$i = 1 + (i-1)d, \qquad je(i,j) = je(i-1, j)d.$$

The first of these equalities involves two possibilities: either $i \neq 1$ and $d = 1$, $e(i,j) = e(i-1, j)$ by the second equation; or $i = 1$. In any case, this proves that for positive i, j we have: $e(i,j) = e(1,j)$. If $1 < j$, then a similar argument, using the symmetry between u and v, proves that $e(i,j) = e(i,1)$. Thus $e(i,j) = e(1,1)$, if both i and j are $\neq 0$. But $e(1,1) = 1$ as a consequence of the choice of v' and thus we have proved:

$$\{u^i v^j\}^f = \{u'^i v'^j\}.$$

If the element x in $\{u, v\}$ is dependent on u, then $x = u^i$ and $f(x; u, u', f) = f(u^i; u, u', f) = u'^i$.—If the element x in $\{u, v\}$ is independent of u, then $x = u^i v^j$ with $j \neq 0$ and

$$\{f(x; u, u', f)\} = \{u'^i v'^j\}, \qquad \{f(x; u, u', f)u'\} = \{u'^{i+1} v'^j\}.$$

Consequently we have:

$$f(x; u, u', f) = (u'^i v'^j)^e, \qquad f(x; u, u', f)u' = (u'^{i+1} v'^j)^d$$

with $e^2 = d^2 = 1$. This implies $je = jd$ or $e = d$, since $j \neq 0$, and $ei + 1 = (i+1)d = (i+1)e$ or $e = d = 1$. Thus we have proved quite generally

$$f(u^i v^j; u, u', f) = u'^i v'^j$$

and this proves (13.1.4) by (13.1.1).

(13.1.5) If u and v are independent elements of infinite order, then $f(x; u, u', f) = f(x; v, v', f)$ for every x in $\{u, v\}$ and for $v' = f(v; u, u', f)$.

It is a consequence of (13.1.2) and (13.1.4) that the two functions $f(x; u, u', f)$ and $f(x; v, v', f)$ are both isomorphisms of $\{u, v\}$ which map u upon u' and v upon v'. This proves their equality.

(13.1.6) $$f(x^i; u, u', f) = f(x; u, u', f)^i.$$

The last statement is a consequence of the fact that $f(\ldots)$ is an iso-

morphism of $F(G)$ upon $F(H)$, if x is an element of finite order. If x is dependent of u, then $x^j = u^d$ and $x^{ij} = u^{id}$ and this proves our equality. If finally x is an independent element of u of infinite order, then our statement is a consequence of (13. 1. 4).

(13. 1. 7) If u and v are elements of infinite order, and if $v' = f(v; u, u', f)$, then

$$f(x; u, u', f) = f(x; v, v', f) \text{ for every } x \text{ in } G.$$

In order to prove this statement let us assume first that u and v are independent elements of infinite order. If x is independent of $\{u, v\}$, then x is independent of u, v and uv. Thus it follows from the "restricted multiplicativity" of $f(\dots)$ mentioned before that

$$f(xuv; u, u', f) = f(x; u, u', f) f(uv; u, u', f) = f(x; u, u', f) u'v'.$$

Consequently

$$f(x; u, u', f) = f(x; uv, u'v', f) .$$

Similarly we have: $f(x; v, v', f) = f(x; uv, u'v', f)$. This proves $f(x; u, u', f) = f(x; v, v', f)$ for elements x which are independent of $\{u, v\}$.

If x is dependent of $\{u, v\}$, then there exists a positive integer i so that $1 \neq x^i$ is an element in $\{u, v\}$. This shows in particular that x is of infinite order. Then it follows from (13. 1. 6) and (13. 1. 5) that

$$f(x; u, u', f)^i = f(x^i; u, u', f) = f(x^i; v, v', f) = f(x; v, v', f)^i.$$

This relation implies $f(x; u, u', f) = f(x; v, v', f)$ since both elements generate the same infinite cyclic group.

Thus (13. 1. 7) has been completely proved for pairs u, v which are independent. If u and v are dependent elements of infinite order, then there exists an element w of infinite order which is independent of both u and v. It follows from what has been proved so far that

$$f(x; u, u', f) = f(x; w, w', f) = f(x; v, v'', f) \text{ for every } x \text{ in } G$$

and for $w' = f(w; u, u', f)$ and $v'' = f(v; w, w', f)$. This implies in particular

$$v' = f(v; u, u', f) = f(v; v, v'', f) = v'' .$$

Consequently we find

$$f(x; u, u', f) = f(x; v, v', f) \text{ for every } x \text{ in } G$$

and this completes the proof of (13. 1. 7).

(13. 1. 8) $f(xy; u, u', f) = f(x; u, u', f) f(y; u, u', f)$ for any x and y in G.

In order to prove this assume first that x and y are independent elements of infinite order. Then it follows from (13. 1. 7) and (13. 1. 4) that

$$f(xy;u,u',f)=f(xy;x,x',f)=f(x;x,x',f)f(y;x,x',f)$$
$$=f(x;u,u',f)f(y;u,u',f).$$

If x and y are not independent elements of infinite order, then there exists an element v of infinite order in G which is independent of $\{x,y\}$. If $\{x,y\}=\{z\}$ is a cyclic group, then $x=z^i$, $y=z^j$ and

$$\begin{aligned} f(xy;u,u',f) &= f(z^{i+j};u,u',f)=f(z;u,u',f)^{i+j} \\ &= f(z^i;u,u',f)f(z^j;u,u',f) \\ &= f(x;u,u',f)f(y;u,u',f) \text{ by } (13.1.6). \end{aligned}$$

If $\{x,y\}$ is not a cyclic group, then there exists a basis w,z of $\{x,y\}$ and we have $x=w^iz^j$, $y=w^hz^k$. Since w and z and v are three independent elements, it follows from the "restricted multiplicativity" of $f(\ldots)$ which has been mentioned before and from (13.1.6) and (13.1.7) that

$$\begin{aligned} f(xy;u,u',f) &= f(w^{i+h}z^{j+k};v,v',f) \\ &= f(w^{i+h};v,v',f)f(z^{j+k};v,v',f) \\ &= f(w;v,v',f)^i f(z;v,v',f)^j f(w;v,v',f)^h f(z;v,v',f)^k \\ &= f(w^i;v,v',f)f(z^j;v,v',f)f(w^h;v,v',f)f(z^k;v,v',f) \\ &= f(x;v,v',f)f(y;v,v',f) \\ &= f(x;u,u',f)f(y;u,u',f)\,. \end{aligned}$$

These relations complete the proof of (13.1.8).

Thus it has been proved that $f(x;u,u',f)$ is a homomorphism of G into H which induces f in the set of cyclic subgroups of G. Consequently f is an isomorphism of G upon the whole group H which induces f in the set of all subgroups of G.

COROLLARY 13.2. *If the abelian group G contains at least two independent elements of infinite order, then every subgroup-isomorphism of G is induced by exactly two (element-)isomorphisms of G.*

This is a consequence of Theorem 13.1 and of (10.1).

COROLLARY 13.3. *If f is an index-preserving subgroup-isomorphism of the abelian group G upon the abelian group H, then f maps every subgroup of G upon an isomorphic subgroup of H and f is therefore strictly index-preserving.*

This is a consequence of Theorems 11.8, 12.3 and 13.1.

THE UNIVERSITY OF ILLINOIS,
URBANA, ILL.

NORMAL SEMI-LINEAR TRANSFORMATIONS.*[1]

By N. Jacobson.

The present paper is devoted to a discussion of vector spaces relative to a totally regular (definite) bilinear form. The coefficients are taken in any quasi-field $\mathfrak{F}$ having an involutorial anti-automorphism. We consider semi-linear transformations (s. l. t.'s) and define the adjoints of such transformations and normality, generalizing the well-known notion due to Toeplitz. It is shown that a normal s. l. t. is always completely reducible and in a number of instances is orthogonally completely reducible in the sense defined in § 2. These cases are (1) any unitary, self-adjoint or skew s. l. t., (2) certain cases where $\mathfrak{F}$ is similar to the real field, the complex field, or the quasi-field of real quaternions. Some of these results may be formulated in a simple fashion as theorems on matrices. In § 9 we re-state the theory in terms of projective geometry.

1. Let $\mathfrak{F}$ be an arbitrary quasi-field with an involutorial anti-automorphism (i. a. a.) $\alpha \to \bar{\alpha}$:[2]

$$\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta} \qquad \overline{\alpha\beta} = \bar{\beta}\bar{\alpha} \qquad \bar{\bar{\alpha}} = \alpha$$

and $\mathfrak{R}$ a vector space of n dimensions over $\mathfrak{F}$. In particular if $\mathfrak{F}$ is commutative we may have $\bar{\alpha} \equiv \alpha$. A bilinear form $f = (x, y)$ is a function of pairs of vectors x, y in $\mathfrak{R}$ with values in $\mathfrak{F}$ such that

$$(x_1 + x_2, y) = (x_1, y) + (x_2, y) \qquad (x, y_1 + y_2) = (x, y_1) + (x, y_2)$$
$$(x, y\alpha) = (x, y)\alpha \qquad (x\alpha, y) = \bar{\alpha}(x, y).$$

If $x_1, x_2, \cdots, x_n$ is a basis for $\mathfrak{R}$ over $\mathfrak{F}$ and $(x_i, x_j) = \alpha_{ij}$, we call $A = (\alpha_{ij})$ the matrix of f relative to $x_1, x_2, \cdots, x_n$. Then for $x = \Sigma x_i \xi_i$ and $y = \Sigma x_i \eta_i$ we have $(x, y) = \Sigma \bar{\xi}_i \alpha_{ij} \eta_j$. Thus f is determined by its matrix and conversely any matrix may be used to define a bilinear form. If we change the basis to

---

* Received May 12, 1938.

[1] Presented to the Society April 15, 1938.

[2] Besides the well-known instances of such quasi-fields we note the following. Let $\mathfrak{D}$ be a domain of integrity with an i. a. a. and suppose $\mathfrak{D}$ has a quotient field $\mathfrak{F}$, i. e. $\mathfrak{F}$ consists of the elements $\alpha\beta^{-1}$, α, β in $\mathfrak{D}$. (Cf. Ore, "Linear equations in non-commutative fields," *Annals of Mathematics*, vol. 32 (1931), p. 466). It is readily verified that $\alpha\beta^{-1} \to \bar{\beta}^{-1}\bar{\alpha}$ is an i. a. a. in $\mathfrak{F}$. For example we may take $\mathfrak{D}$ to be a ring of differential operators and $\bar{\alpha}$ the adjoint of the operator α.

$y_1, y_2, \cdots, y_n$ where $y_i = \Sigma x_j \mu_{ji}$, $M = (\mu_{ij})$ non-singular then the matrix of f relative to $y_1, y_2, \cdots, y_n$ is $\bar{M}'AM$, $M' = (\nu_{ij})$, $\nu_{ij} = \mu_{ji}$.

f is hermitian if $(\overline{x, y}) = (y, x)$, skew-hermitian if $(\overline{x, y}) = -(y, x)$. The conditions on the matrix of f are respectively $\bar{A}' = A$ and $\bar{A}' = -A$. We suppose from now on that one of these cases obtains and in addition that f is *totally-regular* [3] in the sense that $(u, u) = 0$ only if $u = 0$. x and y are said to be orthogonal if $(x, y) = 0$ (or $(y, x) = 0$). If $\mathfrak{S}$ is a subspace the set of vectors y orthogonal to all x in $\mathfrak{S}$ is a subspace $\mathfrak{S}'$ called the orthogonal complement of $\mathfrak{S}$.

Suppose $u_1, u_2, \cdots, u_k$ are vectors such that $(u_i, u_i) = \beta_i \neq 0$ and $(u_i, u_j) = 0$ if $i \neq j$ and let R_k denote the space spanned by the u's. Consider the transformation $\boldsymbol{E}_k$ such that

$$x\boldsymbol{E}_k = \sum_{i=1}^{k} u_i (u_i, u_i)^{-1} (u_i, x).$$

$\boldsymbol{E}_k$ is linear, maps $\mathfrak{R}$ into $\mathfrak{R}_k$, leaves the elements of $\mathfrak{R}_k$ invariant and sends $\mathfrak{R}'_k$ into 0. We call $\boldsymbol{E}_k$ an orthogonal projection of $\mathfrak{R}$ on $\mathfrak{R}_k$. Note also that $(x, y\boldsymbol{E}_k) = (x\boldsymbol{E}_k, y)$ and hence $\boldsymbol{1} - \boldsymbol{E}_k$ is an orthogonal projection on $\mathfrak{R}'_k$. For any x we have $x = x\boldsymbol{E}_k + x(\boldsymbol{1} - \boldsymbol{E}_k) = x_k + x'_k$ where $x_k \in \mathfrak{R}_k$, $x'_k \in \mathfrak{R}'_k$. Hence $\mathfrak{R} = \mathfrak{R}_k + \mathfrak{R}'_k$, $\mathfrak{R}_k \cap \mathfrak{R}'_k = 0$.[4] If $\mathfrak{R}_k \neq \mathfrak{R}$ we may choose a vector of the form $x(\boldsymbol{1} - \boldsymbol{E}_k) \neq 0$ and using it as u_{k+1} we obtain $u_1, u_2, \cdots, u_{k+1}$ such that $(u_i, u_i) = \beta_i \neq 0$ and $(u_i, u_j) = 0$ if $i \neq j$. If we begin with any vector $\neq 0$ as u_1 we obtain a basis of this type, called orthogonal, for the whole space. If $\mathfrak{S}$ is any subspace we may obtain an orthogonal basis $v_1, v_2, \cdots, v_r$ for $\mathfrak{S}$ and supplement it with $v_{r+1}, v_{r+2}, \cdots, v_n$ to obtain an orthogonal basis for $\mathfrak{R}$. $v_{r+1}, v_{r+2}, \cdots, v_n$ generate $\mathfrak{S}'$ and hence $\mathfrak{R} = \mathfrak{S} + \mathfrak{S}'$, $\mathfrak{S} \cap \mathfrak{S}' = 0$. We write $\mathfrak{R} = \mathfrak{S} \oplus \mathfrak{S}'$ in place of these two equations.

Let $\mathfrak{L}$ denote the lattice of subspaces of $\mathfrak{R}$. The correspondence $\mathfrak{S} \to \mathfrak{S}'$ is $(1-1)$ and involutorial, $\mathfrak{S}'' = \mathfrak{S}$. We note also that it is an anti-automorphism of $\mathfrak{L}$, i.e.,

$$(\mathfrak{S}_1 + \mathfrak{S}_2)' = \mathfrak{S}_1' \cap \mathfrak{S}_2' \qquad (\mathfrak{S}_1 \cap \mathfrak{S}_2)' = \mathfrak{S}'_1 + \mathfrak{S}'_2.$$ [5]

If $\mathfrak{R} = \mathfrak{R}_1 + \mathfrak{R}_2 + \cdots + \mathfrak{R}_l$ where $\mathfrak{R}_i \neq 0$ and $\mathfrak{R}_i \subset \mathfrak{R}'_j$ if $i \neq j$ then we write $\mathfrak{R} = \mathfrak{R}_1 \oplus \mathfrak{R}_2 \oplus \cdots \oplus \mathfrak{R}_l$. It follows that every vector is ex-

[3] Cf. Weyl, "On generalized Riemann matrices," *Annals of Mathematics*, vol. 35 (1934), p. 715 and Birkhoff and v. Neumann, "The logic of quantum mechanics," *Annals of Mathematics*, vol. 37 (1936), pp. 823-843. Evidently the assumption of total-regularity excludes the case $\mathfrak{F}$ commutative, $\bar{a} \equiv a$ and f skew.

[4] It follows that $\boldsymbol{E}_k$ is the only orthogonal projection of $\mathfrak{R}$ on $\mathfrak{R}_k$.

[5] Cf. Birkhoff and v. Neumann, *loc. cit.* in 3.

pressible uniquely in the form $x_1 + x_2 + \cdots + x_l$, $x_i \in \mathfrak{R}_i$. If $u_i^{(1)}$, $u_i^{(2)}, \cdots, u_i^{(n_i)}$ is an orthogonal basis for $\mathfrak{R}_i$ then the $u_i^{(j)}$, $i = 1, \cdots, l$: $j = 1, \cdots, n_i$ form an orthogonal basis for $\mathfrak{R}$.

2. We recall the definition of a semi-linear transformation (s. l. t.) $\boldsymbol{T}$ with automorphism S as a single valued mapping of $\mathfrak{R}$ on itself such that

$$(x + y)\boldsymbol{T} = x\boldsymbol{T} + y\boldsymbol{T} \qquad (x\alpha)\boldsymbol{T} = (x\boldsymbol{T})\alpha^S.$$

If $x_i\boldsymbol{T} = \Sigma x_j \tau_{ji}$ and $x = \Sigma x_i \xi_i$ then $x\boldsymbol{T} = \Sigma x_i \tau_{ij} \xi_j^S$. $\boldsymbol{T}$ is determined by the matrix $T = (\tau_{ij})$ and by the automorphism S. If $\mathfrak{S}$ is a subspace then $\mathfrak{S}\boldsymbol{T}$ the set of vectors of the form $y\boldsymbol{T}$, $y \in \mathfrak{S}$ is a subspace also. The sum of two s. l. t.'s with the same automorphism is another such s. l. t. If $\boldsymbol{T}_1$ and $\boldsymbol{T}_2$ have respectively the matrices T_1 and T_2 and the automorphisms S_1 and S_2 then $\boldsymbol{T}_1\boldsymbol{T}_2$ is an s. l. t. with matrix $T_2 T_1^{S_2}$ and automorphism $S_1 S_2$. The scalar multiplication $x \rightarrow x\mu = x\boldsymbol{M}$ is an s. l. t. with matrix 1μ and automorphism $\alpha \rightarrow \mu^{-1}\alpha\mu$. If $y_1, y_2, \cdots, y_n$ is a basis such that $y_i = \Sigma x_j \mu_{ji}$, the matrix of $\boldsymbol{T}$ relative to the y's is $M^{-1}TM^S$, $M = (\mu_{ij})$.[6]

If Ω is a set of s. l. t.'s then the system of subspaces invariant under all s. l. t.'s of Ω is a sublattice $\mathfrak{L}(\Omega)$ of $\mathfrak{L}$. $\mathfrak{S}$ in $\mathfrak{L}(\Omega)$ is irreducible if it contains no proper invariant subspace. We recall also that $\mathfrak{L}(\Omega)$ or Ω is completely reducible if for every $\mathfrak{S}_1$ in $\mathfrak{L}(\Omega)$ there is an $\mathfrak{S}_2$ in this lattice such that $\mathfrak{R} = \mathfrak{S}_1 + \mathfrak{S}_2$, $\mathfrak{S}_1 \cap \mathfrak{S}_2 = 0$. In view of the chain conditions this is equivalent, as is well-known, to the condition $\mathfrak{R} = \mathfrak{R}_1 + \mathfrak{R}_2 + \cdots + \mathfrak{R}_l$, where the $\mathfrak{R}_i$ are irreducible.[7] Ω is *orthogonally completely reducible* if $\mathfrak{L}(\Omega) \supset \mathfrak{S}'$ for every $\mathfrak{S}$ in $\mathfrak{L}(\Omega)$. If $\{\Omega_a\}$ is a set of sets of s. l. t.'s and Ω the logical sum of the Ω_a then $\mathfrak{L}(\Omega)$ is the intersection $\Delta\mathfrak{L}(\Omega_a)$. Hence it follows directly from the definition that if each Ω_a is orthogonally completely reducible, then so is Ω.

Now suppose $\mathfrak{L}(\Omega) \supset \mathfrak{S}'$ for every irreducible $\mathfrak{S}$ in this lattice and let $\mathfrak{U}$ be arbitrary in $\mathfrak{L}(\Omega)$. Suppose $\mathfrak{U} \supset \mathfrak{S}_1$ irreducible in $\mathfrak{L}(\Omega)$. Then $\mathfrak{U} \cap \mathfrak{S}'_1 = \mathfrak{U}_1 \in \mathfrak{L}(\Omega)$ and $\mathfrak{U} = \mathfrak{U} \cap \mathfrak{R} = \mathfrak{U} \cap (\mathfrak{S}_1 \oplus \mathfrak{S}'_1) = \mathfrak{S}_1 \oplus \mathfrak{U}_1$.[8] If $\mathfrak{U}_1$ is not reducible we repeat this process and obtain $\mathfrak{U}_1 = \mathfrak{S}_2 \oplus \mathfrak{U}_2$ where $\mathfrak{S}_2, \mathfrak{U}_2 \in \mathfrak{L}(\Omega)$ and $\mathfrak{S}_2$ is irreducible. Then $\mathfrak{U} = \mathfrak{S}_1 \oplus \mathfrak{S}_2 \oplus \mathfrak{U}_2$. Continuing in this way we obtain $\mathfrak{U} = \mathfrak{S}_1 \oplus \mathfrak{S}_2 \oplus \cdots \oplus \mathfrak{S}_k$, $\mathfrak{S}_i$ irreducible in

---

[6] Cf. Jacobson, "Pseudo-linear transformations," *Annals of Mathematics*, vol. 38 (1937), pp. 484-507 for the results of this paragraph.

[7] See for example van der Waerden's *Moderne Algebra I*, 1st ed., p. 143, or 2nd ed., p. 155.

[8] We are applying the rule that if $\mathfrak{S}_1 \supset \mathfrak{S}_2$ then

$$\mathfrak{S}_1 \cap (\mathfrak{S}_2 + \mathfrak{S}_3) = \mathfrak{S}_2 + (\mathfrak{S}_1 \cap \mathfrak{S}_3).$$

$\mathfrak{L}(\Omega)$. It follows that $\mathfrak{U}' = \mathfrak{S}'_1 \cap \mathfrak{S}'_2 \cap \cdots \cap \mathfrak{S}'_k \in \mathfrak{L}(\Omega)$ and hence Ω is orthogonally completely reducible. If we apply this process to $\mathfrak{R}$ we obtain $\mathfrak{R} = \mathfrak{R}_1 \oplus \mathfrak{R}_2 \oplus \cdots + \mathfrak{R}_l$ where the $\mathfrak{R}_i$ are irreducible in $\mathfrak{L}(\Omega)$.[9] Hence we obtain an orthogonal basis for $\mathfrak{R}$ relative to which all the s. l. t.'s in Ω have the form

$$\begin{pmatrix} T_1 & & & & \\ & T_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & T_l \end{pmatrix}$$

where the system T_i is irreducible.

3. If $\boldsymbol{T}$ is any single valued mapping of R into itself, S an automorphism, we define an *S-adjoint* $\boldsymbol{T}_S$ of $\boldsymbol{T}$ as a transformation such that

$$(x, y\boldsymbol{T})^S = (x\boldsymbol{T}_S, y) \tag{1}$$

for all x and y. If $\boldsymbol{T}_S{}^{(1)}$ and $\boldsymbol{T}_S{}^{(2)}$ are two such transformations then $(x\boldsymbol{T}_S{}^{(1)}, y) = (x\boldsymbol{T}_S{}^{(2)}, y)$ and hence $(x\boldsymbol{T}_S{}^{(1)} - x\boldsymbol{T}_S{}^{(2)}, y) = 0$ and $x\boldsymbol{T}_S{}^{(1)} = x\boldsymbol{T}_S{}^{(2)}$. Thus if $\boldsymbol{T}_S$ exists it is single valued and unique. Since

$$\begin{aligned}((x_1 + x_2)\boldsymbol{T}_S, y) = (x_1 + x_2, y\boldsymbol{T})^S &= (x_1, y\boldsymbol{T})^S + (x_2, y\boldsymbol{T})^S \\ &= (x_1\boldsymbol{T}_S, y) + (x_2\boldsymbol{T}_S, y) = (x_1\boldsymbol{T}_S + x_2\boldsymbol{T}_S, y),\end{aligned}$$

$(x_1 + x_2)\boldsymbol{T}_S = x_1\boldsymbol{T}_S + x_2\boldsymbol{T}_S$. Similarly we obtain $\alpha\boldsymbol{T}_S = \boldsymbol{T}_S\alpha^{\bar{S}}$ where α is the scalar multiplication $x \to x\alpha$ and $\bar{S}$ is the automorphism $\alpha \to \overline{\bar{\alpha}^S} \equiv \alpha^{\bar{S}}$. Thus $\boldsymbol{T}_S$ is an s. l. t. with automorphism $\bar{S}$. From (1) we obtain $(x, y\boldsymbol{T}_S)^{\bar{S}^{-1}} = (x\boldsymbol{T}, y)$. Hence $\boldsymbol{T}$ is the $\bar{S}^{-1}$ adjoint of $\boldsymbol{T}_S$ if $\boldsymbol{T}_S$ exists and a necessary condition that $\boldsymbol{T}_S$ exist is therefore that $\boldsymbol{T}$ be a s. l. t. with automorphism $S^{-1} = \overline{\bar{S}^{-1}}$. This condition is also sufficient. For let $\boldsymbol{T}_S$ be the s. l. t. with matrix $T^* = A^{-1}(\bar{T}')^{\bar{S}}A^{\bar{S}}$ (T the matrix of $\boldsymbol{T}$ and A that of the bilinear form relative to the basis $x_1, x_2, \cdots, x_n$) and automorphism S. Then

$$\begin{aligned}(xy\boldsymbol{T})^S &= (\Sigma x_i\xi_i, \Sigma x_j\tau_{ja}\eta_a{}^{S^{-1}})^S = \Sigma\bar{\xi}_i{}^S\alpha_{ij}{}^S\tau_{ja}{}^S\eta_a \\ (x\boldsymbol{T}_S, y) &= (\Sigma x_a\tau^*{}_{ai}\xi_i{}^{\bar{S}}, \Sigma x_j\eta_j) = \Sigma\overline{\xi_i{}^{\bar{S}}}\bar{\tau}^*{}_{ai}\alpha_{aj}\eta_j \\ &= \Sigma\bar{\xi}_i{}^S\bar{\tau}^*{}_{ai}\alpha_{aj}\eta_j\end{aligned}$$

and $(x\boldsymbol{T}_S, y) = (x, y\boldsymbol{T})^S$ since $\overline{T^{*\prime}}A = A^S T^S$. We call $\boldsymbol{T}_S$ the *adjoint* of T

---

[9] The converse does not hold. There exist Ω's for which $\mathfrak{R} = \mathfrak{R}_1 \oplus \cdots \oplus \mathfrak{R}_l$ where the $\mathfrak{R}_i$ are irreducible but Ω is not orthogonally completely reducible.

and denote it more simply as T^*. The relation is a symmetric one: $T^{**} = T$. If T_1 and T_2 are two s. l. t.'s with automorphisms S_1^{-1} and S_2^{-1}, then

$$(x, yT_1T_2)^{S_2S_1} = (xT^*_2, yT_1)^{S_1} = (xT^*_2T^*_1, y),$$

i.e., $(T_1T_2)^* = T^*_2T^*_1$. If $S_1 = S_2 = S$ then

$$(x, y)(T_1 + T_2))^S = (x, yT_1)^S + (x, yT_2)^S = (x(T^*_1 + T^*_2), y)$$

or $(T_1 + T_2)^* = T^*_1 + T^*_2$. We note finally that if M is the s. l. t. $x \to x\mu$ then M^* is the s. l. t. $x \to x\bar{\mu}$ since $\mu(x, y\mu)\mu^{-1} = (x\bar{\mu}, y)$.[10]

Let Ω be a set of s. l. t.'s and Ω^* the set consisting of the adjoints of the transformations in Ω. It is readily seen that if $\mathfrak{S} \epsilon \mathfrak{L}(\Omega)$ then $\mathfrak{S}' \epsilon \mathfrak{L}(\Omega^*)$. Hence $\mathfrak{L}(\Omega)$ and $\mathfrak{L}(\Omega^*)$ are anti-isomorphic. The condition that $\mathfrak{L}(\Omega)$ be orthogonally completely reducible is that $\mathfrak{L}(\Omega) = \mathfrak{L}(\Omega^*)$ and hence we have the theorem:

THEOREM 1. *If Ω is a set of semi-linear transformations containing the adjoint T^* of every T in Ω, then Ω is orthogonally completely reducible.*

4. T is a *normal* s. l. t. if $T^*T = TT^*$. Evidently if T is normal so is T^* and if T_1 and T_2 are normal and $T_1T_2 = T_2T_1$, $T_1T^*_2 = T^*_2T_1$ then T_1T_2 is normal. In particular the powers of a normal s. l. t. are normal. Special cases of normal s. l. t.'s are T *self-adjoint* where $T^* = T$, T *skew* where $T^* = -T$ and T *unitary* where $TT^* = T^*T = 1$.

Suppose T is normal and z is a vector such that $zT = 0$. Then $(zT^*, zT^*) = (z, zT^*T)^S = (z, zTT^*)^S = 0$ and hence $zT^* = 0$. If $\mathfrak{S} \epsilon \mathfrak{L}(T)$, $\mathfrak{S}T^* \epsilon \mathfrak{L}(T)$ also. Suppose $\mathfrak{S}$ is irreducible. Then either $\mathfrak{S}T = \mathfrak{S}T^* = 0$ or the mapping $y \to yT^*$ is $(1-1)$ from $\mathfrak{S}$ to $\mathfrak{S}T^*$. It follows that any invariant subspace of $\mathfrak{S}T^*$ has the form $\mathfrak{U}T^*$ where $\mathfrak{U}$ is invariant in $\mathfrak{L}(T)$. Hence $\mathfrak{U}T^*$ can not be proper. Thus in any case if $\mathfrak{S}$ is irreducible either $\mathfrak{S}T^* = 0$ or $\mathfrak{S}T^*$ is irreducible. If T^* is linear (l. t.) $\mathfrak{S}T^* \neq 0$ is similar to $\mathfrak{S}$.

Let $\mathfrak{R}_0$ be the join of all irreducible subspaces $\mathfrak{S}$ of $\mathfrak{L}(T)$. $\mathfrak{R}_0$ is invariant under T^* and hence $\mathfrak{R}'_0 \epsilon \mathfrak{L}(T)$. If $\mathfrak{R}'_0 \neq 0$, it contains $\mathfrak{S}_0 \neq 0$ which is irreducible in $\mathfrak{L}(T)$. But this is impossible since $\mathfrak{R}_0 \cap \mathfrak{R}'_0 = 0$. Thus $\mathfrak{R}'_0 = 0$, i. e., $\mathfrak{R} = \mathfrak{R}_0$. $\mathfrak{R}$ is a join of irreducible invariant subspaces and hence is a join of a finite number of such subspaces. We therefore have

[10] This discussion is valid for any non-degenerate hermitian or skew-hermitian form. No use has been made of the total-regularity of f.

THEOREM 2. *Any normal s. l. t. is completely reducible.*

Remark. It is readily seen that the above proof holds also under the weaker assumption that $TT^* = T^*T\mu$, $\mu \neq 0$ in S.

5. In the remainder of the paper we discuss some special conditions that a normal s. l. t. be orthogonally completely reducible. If $T^* = \pm T$ then any subspace $\mathfrak{S}$ invariant under T is invariant under T^*. Hence $\mathfrak{S}' \epsilon \mathfrak{L}(T)$. If $T^*T = TT^* = 1$ then $\mathfrak{S}T$ is an invariant subspace of $\mathfrak{S}$ and since T is non-singular $\mathfrak{S}T = \mathfrak{S}$ and $\mathfrak{S}T^* = \mathfrak{S}T^{-1} = \mathfrak{S}$. Thus $\mathfrak{S}' \epsilon \mathfrak{L}(T)$ in this case also and we have the theorem:

THEOREM 3. *Any symmetric, skew or unitary semi-linear transformation is orthogonally completely reducible.*

If T is any s. l. t. with automorphism S^{-1} we define the ring $\mathfrak{F}[t, S^{-1}]$ as the ring of polynomials in the indeterminate t with coefficients in $\mathfrak{F}$ such that $\alpha t = t\alpha^{S^{-1}}$ or $t\alpha = \alpha^S t$. Then any irreducible invariant subspace $\mathfrak{S}$ of T is generated by a single vector x such that

$$x\phi(T) = xT^r - xT^{r-1}\beta_1 - \cdots - x\beta_r = 0$$

and $\phi(t) = t^r - t^{r-1}\beta_1 - \cdots - \beta_r$ is irreducible in $\mathfrak{F}[t, S^{-1}]$.[11] The condition that two such spaces be similar is that the corresponding polynomials be similar in the sense of Ore.

6. Suppose now that $\mathfrak{F}$ is a commutative real closed field[12] and $\bar{\alpha} \equiv \alpha$. If $x_1, x_2, \cdots, x_n$ is an orthogonal basis for $\mathfrak{R}$ then either $(x_i, x_i) > 0$ for all i or $(x_i, x_i) < 0$ (in the algebraic ordering of $\mathfrak{F}$). For if $(x_1, x_1) = \beta_1 > 0$ and $(x_2, x_2) = \beta_2 < 0$ then $(z, z) = 0$ if $z = x_1 + x_2\lambda$, $\lambda = (-\beta_1/\beta_2)^{\frac{1}{2}}$. If we replace f by $-f$ we do not change the definition of the adjoint. Hence we may suppose that f is positive definite: $(x_i, x_i) = \beta_i > 0$. By replacing x_i by $x_i\beta_i^{-\frac{1}{2}} = u_i$ we obtain a basis such that $(u_i, u_j) = \delta_{ij}$. A basis of this type will be called *Cartesian.* It is clear from the computation of § 1 that the passage from one Cartesian basis to another is given by an orthogonal matrix $M(MM' = M'M = 1)$.

If T is an l. t. with matrix T relative to the Cartesian basis $u_1, u_2, \cdots, u_n$, T^* has the matrix T' relative to this basis. T is normal if and only if $TT' = T'T$ and T is orthogonal (unitary), self-adjoint or skew according as

[11] Jacobson, *loc. cit.* in 6.

[12] In the sense of Artin-Schreier. Cf. van der Waerden, *Moderne Algebra I*, p. 227, 1st ed., or p. 235, 2nd ed.

T is orthogonal, symmetric or skew. Let $\mathfrak{R}_1$ be the join of all irreducible invariant subspaces similar to a given one and suppose $\mathfrak{R}_1\boldsymbol{T} \neq 0$. As above $\mathfrak{R}_1$ is also in $\mathfrak{L}(\boldsymbol{T}^*)$ and hence in $\mathfrak{L}(\boldsymbol{L})$, where $\boldsymbol{L} = \boldsymbol{TT}^* = \boldsymbol{T}^*\boldsymbol{T}$. We may decompose $\mathfrak{R}_1$ as $\mathfrak{S}^{(1)} + \cdots + \mathfrak{S}^{(k)}$ where $\mathfrak{S}^{(i)}$ consists of all vectors y_i such that $y_i\boldsymbol{L} = y_i\alpha_i$, $\alpha_i > 0$.[13] $\boldsymbol{T}$ acting in $\mathfrak{S}^{(i)}$ has the form $\beta_i\boldsymbol{O}_i$ where $\boldsymbol{O}_i$ is orthogonal and $\beta_i = \alpha_i^{\frac{1}{2}}$. If $\mathfrak{S}_1{}^{(i)}$ and $\mathfrak{S}_1{}^{(j)}$ are irreducible elements of $L(\boldsymbol{T})$ contained in $\mathfrak{S}^{(i)}$ and $\mathfrak{S}^{(j)}$ respectively and T_i and T_j the matrices of $\boldsymbol{T}$ relative to orthogonal bases in these spaces, $T_i = \beta_i O_i$, $T_j = \beta_j O_j$, O_i and O_j orthogonal. Since $S^{-1}T_iS = T_j$, $S^{-1}O_iS = O_j\beta_j\beta_i^{-1}$ and since the roots of an orthogonal matrix have absolute value 1 this implies that $\beta_i = \beta_j$. Thus $\boldsymbol{T}$ acting in $\mathfrak{R}_1$ is a positive multiple of an orthogonal l. t. If $\mathfrak{S}_1$ is any irreducible subspace in $\mathfrak{L}(\boldsymbol{T})$ either $\mathfrak{S}_1\boldsymbol{T} = \mathfrak{S}_1\boldsymbol{T}^* = 0$ or $\mathfrak{S}_1$ can be embedded in a space $\mathfrak{R}_1$. It follows that $\mathfrak{S}_1$ is also invariant under $\boldsymbol{T}^*$ and by the remarks of § 2 we have

THEOREM 4. *If $\boldsymbol{T}$ is a normal linear transformation in $\mathfrak{R}$ over a real closed field $\mathfrak{F}$, $\boldsymbol{T}$ is orthogonally completely reducible.*

Now by Theorem 4 we may write $\mathfrak{R} = \mathfrak{S}_1 \oplus \mathfrak{S}_2 \oplus \cdots \oplus \mathfrak{S}_l$ where the $\mathfrak{S}_i$ are irreducible and invariant with respect to T and hence are either 1 or 2-dimensional since the irreducible polynomials in $\mathfrak{F}[t]$ have degree 1 or 2. If we choose Cartesian bases in the spaces $\mathfrak{S}_i$ we obtain such a basis for $\mathfrak{R}$ and relative to this basis the matrix of $\boldsymbol{T}$ has the completely reduced form

$$(2) \qquad \begin{bmatrix} T_1 & & & & \\ & T_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & T_l \end{bmatrix}$$

We therefore have the following theorem due to Murnaghan and Wintner:[14]

THEOREM 5. *If $\boldsymbol{T}$ is a normal matrix with elements in a real closed field then there exists an orthogonal matrix M such that $M^{-1}TM = M'TM$ has the form* (2) *where the T_i are one and two dimensional.*

---

[13] If $\boldsymbol{L}$ is a self-adjoint l. t. a simple computation shows that its characteristic roots are real. If $\mathfrak{S}$ is the set of vectors u such that $u\boldsymbol{L} = u\alpha$ the space orthogonal to $\mathfrak{S}$ is also invariant under $\boldsymbol{L}$ and hence if we continue this process we obtain the decomposition. If $\boldsymbol{L} = \boldsymbol{TT}^*$, $\alpha(u, u) = (u\boldsymbol{TT}^*, u) = (u\boldsymbol{T}, u\boldsymbol{T}) \geqq 0$ and hence $\alpha \geqq 0$.

[14] "A canonical form for real matrices under orthogonal transformations," *Proceedings of the National Academy of Sciences*, vol. 17 (1931), pp. 417-420.

By changing the sign of one of the vectors if necessary we may suppose that M is proper, i. e., det $M = 1$.

As has been shown by Murnaghan and Wintner the condition that a two dimensional matrix be normal is that it be symmetric or have the form

$$\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \tag{3}$$

where $\beta \neq 0$. If T is symmetric it is well known that it can be transformed into diagonal form by an orthogonal matrix and conversely. Thus the matrices (3) constitute the set of irreducible 2-rowed normal matrices. Note that $TT' = 1\gamma$, $\gamma = \alpha^2 + \beta^2 \neq 0$ and hence T is a positive multiple of an orthogonal matrix O as was shown in the proof of Theorem 4.

THEOREM 6. *T is an irreducible normal matrix if and only if it is 1-rowed or a positive multiple of a 2-rowed orthogonal non-symmetric matrix O.*

If T is symmetric, skew orthogonal then O is respectively symmetric skew or orthogonal and Theorems 5 and 6 give the well-known results on the orthogonal reduction of these matrices.

7. Let $\mathfrak{F} = \mathfrak{F}_0(\sqrt{-1})$ where $\mathfrak{F}_0$ is real closed and $\bar{\alpha} = \alpha_0 - \sqrt{-1}\beta_0$ for $\alpha = \alpha_0 + \sqrt{-1}\beta_0$. $\mathfrak{F}$ is algebraically closed. If f is a skew hermitian form, $\sqrt{-1}f$ is hermitian. Hence as in § 6 we may suppose that f is hermitian and positive definite. Then $\mathfrak{R}$ has a *unitary* basis $u_1, u_2, \cdots, u_n$, i. e., $(u_i, u_j) = \delta_{ij}$. The change to a second unitary basis is given by a unitary matrix M $(\bar{M}'M = M\bar{M}' = 1)$.

An l. t. $\boldsymbol{T}$ is normal if and only if $\bar{T}'T = T\bar{T}'$ for the matrix T of $\boldsymbol{T}$ relative to a unitary basis. Since $\mathfrak{F}$ is algebraically closed the irreducible invariant subspaces of $\boldsymbol{T}$ are one dimensional. Hence, as before, we obtain orthogonal complete reducibility and hence the following theorem of Toeplitz:[15]

THEOREM 7. *If T is a normal matrix with elements in $\mathfrak{F} = \mathfrak{F}_0(\sqrt{-1})$, $\mathfrak{F}_0$ real closed, then there exists a unitary matrix M such that $M^{-1}TM = \bar{M}'TM$ is diagonal.*

If T is hermitian, skew hermitian or unitary, the diagonal elements of the normal form are respectively real, pure imaginary or of absolute value $= 1$.

We consider next the anti-linear transformations (a. l. t.) in $\mathfrak{R}$. These are the s. l. t.'s $\boldsymbol{T}$ with automorphisms S such that $\alpha^S = \bar{\alpha}$. Let T be the matrix of $\boldsymbol{T}$ relative to a unitary basis. The computation on p. 48 shows that

[15] Toeplitz, "Das algebraische Analogon zu einen Satze von Fejér," *Mathematische Zeitschrift*, Bd. 2 (1918), pp. 187-197.

$\boldsymbol{T}^*$ has the matrix T' and automorphism S ($S^2 = E$). We write $\boldsymbol{T} = (T, S)$ and $\boldsymbol{T}^* = (T', S)$. Then $\boldsymbol{T}^*\boldsymbol{T}$ and $\boldsymbol{T}\boldsymbol{T}^*$ are l. t.'s with matrices $T\bar{T}'$ and $T'\bar{T}$ respectively. The condition that $\boldsymbol{T}$ be normal is $T\bar{T}' = T'\bar{T} = \overline{\bar{T}'T}$. $\boldsymbol{T}$ is self-adjoint, skew or unitary if and only if T is symmetric, skew or unitary.

$\boldsymbol{T}\boldsymbol{T}^*$ is a self-adjoint l. t. In an invariant subspace of this l. t. we can choose a unitary basis of vectors u such that $u\boldsymbol{T}\boldsymbol{T}^* = u\alpha$. Then $\bar{\alpha}(u, u) = (u\boldsymbol{T}\boldsymbol{T}^*, u) = (u\boldsymbol{T}, u\boldsymbol{T}) = (u\boldsymbol{T}, u\boldsymbol{T}) \geqq 0$ and $\bar{\alpha} = \alpha \geqq 0$.

Now suppose that $\mathfrak{S}_1$ is irreducible and invariant relative to $\boldsymbol{T}$. If $\mathfrak{S}_1\boldsymbol{T} = 0$, $\mathfrak{S}_1\boldsymbol{T}^* = 0$ also. Hence suppose $\mathfrak{S}_1\boldsymbol{T} = \mathfrak{S}_1$. Then $\mathfrak{S}_1\boldsymbol{T}^2 = \mathfrak{S}_1$ and since $\boldsymbol{T}^2$ is a normal l. t. by the above, $\mathfrak{S}_1(\boldsymbol{T}^*)^2 = \mathfrak{S}_1$. Set $\boldsymbol{L} = \boldsymbol{T}\boldsymbol{T}^* = \boldsymbol{T}^*\boldsymbol{T}$, $\boldsymbol{L}^2 = \boldsymbol{T}^2(\boldsymbol{T}^*)^2 = (\boldsymbol{T}\boldsymbol{T}^*)^2$. The space $\mathfrak{R}_1 = \mathfrak{S}_1 + \mathfrak{S}_1\boldsymbol{T}^* = \mathfrak{S}_1 + \mathfrak{S}_1\boldsymbol{L}$ is invariant relative to $\boldsymbol{T}$ and $\boldsymbol{T}^*$. If $y_1 \neq 0$ is a vector in $\mathfrak{S}_1$ such that $y_1\boldsymbol{L}^2 = y_1\alpha$, ($\alpha > 0$), then since every vector in $\mathfrak{S}_1$ has the form $y_1\mu(\boldsymbol{T})$ and $\boldsymbol{L}^2\mu(\boldsymbol{T}) = \mu(\boldsymbol{T})\boldsymbol{L}^2$, $\alpha\mu(\boldsymbol{T}) = \mu(\boldsymbol{T})\alpha$, we have $y_1\boldsymbol{L}^2 = y_1\alpha$ for every y_1 in $\mathfrak{S}_1$. Then $y_2\boldsymbol{L}^2 = y_2\alpha$ for every y_2 in $\mathfrak{S}_1\boldsymbol{T}^*$ and $x_1\boldsymbol{L}^2 = x_1\alpha$ for all x_1 in $\mathfrak{R}_1$. If $x_1\boldsymbol{L} = x_1\beta$, $\beta > 0$ and hence $\beta = \alpha^{\frac{1}{2}}$. It follows that $x_1\boldsymbol{L} = x_1\beta$ for all x_1 in $\mathfrak{R}_1$. Then $\mathfrak{S}_1\boldsymbol{T}^* = \mathfrak{S}_1\boldsymbol{L} = \mathfrak{S}_1 \epsilon \mathfrak{L}(\boldsymbol{T}^*)$. We therefore have the following theorem:

THEOREM 8. *If $\boldsymbol{T}$ is a normal anti-linear transformation in $\mathfrak{R}$ over $\mathfrak{F} = \mathfrak{F}_0(\sqrt{-1})$ and $\mathfrak{F}_0$ real closed, then $\boldsymbol{T}$ is orthogonally completely reducible.*

If $\boldsymbol{T}$ is irreducible $\mathfrak{R}$ is 1- or 2-dimensional.[16] Evidently any a. l. t. in 1-dimensions is normal. If $\boldsymbol{T} = 1\tau$, $\tau = \beta\epsilon$ where $\beta \geqq 0$ and $\epsilon\bar{\epsilon} = 1$. Thus $\boldsymbol{T}$ is a non-negative multiple of a unitary a. l. t. Suppose next that $\mathfrak{R}$ is 2-dimensional. We have seen that a necessary condition for irreducibility is that $\boldsymbol{T}\boldsymbol{T}^* = 1\beta = \boldsymbol{T}^*\boldsymbol{T}$, $\beta > 0$ and hence $\boldsymbol{T} = \gamma\boldsymbol{U}$, $\gamma = \beta^{\frac{1}{2}}$ and $\boldsymbol{U}$ is unitary. If $\boldsymbol{T}^* = \boldsymbol{T}$, $\boldsymbol{T}^2 = \beta$ and if x is any vector and $\gamma = \beta^{\frac{1}{2}}$, $y = x\boldsymbol{T} + x\gamma$ then $y\boldsymbol{T} = y\gamma$. Thus either y or x is an invariant vector $\neq 0$, contrary to the irreducibility of $\boldsymbol{T}$. Suppose conversely that $\boldsymbol{T} = \gamma\boldsymbol{U}$ and $\boldsymbol{T}$ is not self-adjoint. $\boldsymbol{T}$ is evidently normal. If $\boldsymbol{T}$ is reducible, then there is a unitary basis u, v such that $u\boldsymbol{T} = u\mu$, $v\boldsymbol{T} = v\nu$. It follows readily that $\boldsymbol{T}$ is self-adjoint. We have therefore proved

THEOREM 9. *If $\boldsymbol{T}$ is an irreducible normal anti-linear transformation, $\mathfrak{R}$ is 1- or 2-dimensional. In the former case $\boldsymbol{T}$ is arbitrary and in the latter, $\boldsymbol{T}$ is a positive multiple of a unitary a. l. t. and is not self-adjoint and conversely.*

---

[16] Asano and Nakayama, "Über halblineare Transformationen," *Mathematische Annalen*, Bd. 115 (1937), p. 110.

Note that $\boldsymbol{U}$ and γ are uniquely determined by $\boldsymbol{T}$ if $\gamma > 0$. For if $\boldsymbol{T} = \gamma \boldsymbol{U} = \gamma_1 \boldsymbol{U}_1$, $\gamma\gamma_1^{-1}$ is unitary and hence $\gamma = \gamma_1$, $\boldsymbol{U} = \boldsymbol{U}_1$.

If $\boldsymbol{T}$ is any normal a. l. t. and $\mathfrak{R} = \mathfrak{R}_1 \oplus \mathfrak{R}_2 \oplus \cdots \oplus \mathfrak{R}_l$ where the $\mathfrak{R}_i$ are irreducible we may choose a unitary basis in each $\mathfrak{R}_i$. The new matrix of $\boldsymbol{T}$ will be $M^{-1}T\bar{M} = N'TN$ where M and N are unitary and $N = \bar{M}$. $M^{-1}T\bar{M}$ will be completely reduced. Hence we have the following theorem:

Theorem 10. *If T is a matrix with elements in $\mathfrak{F} = \mathfrak{F}_0(\sqrt{-1})$, $\mathfrak{F}_0$ real closed and $T\bar{T}' = T'\bar{T}$, then there exists a unitary matrix M such that*

$$(4) \qquad M^{-1}T\bar{M} = N'TN = \begin{bmatrix} T_1 & & & & \\ & T_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & T_l \end{bmatrix}, \quad N = \bar{M}$$

where T_i is either 1-rowed or a positive multiple of a 2-rowed unitary matrix which is not symmetric.

We may, of course, re-arrange the T_i's in an arbitrary manner without destroying the validity of the result.

Corollary 1. *If T is a symmetric matrix with elements in $\mathfrak{F}_0(\sqrt{-1})$, there exists a unitary matrix M such that $D = M^{-1}T\bar{M} = N'TN$ is diagonal.*

If D has diagonal elements $\delta_i = \beta_i\epsilon_i$, $\beta_i \geq 0$, $\epsilon_i\bar{\epsilon}_i = 1$, we may replace M by the unitary matrix MQ where Q is the diagonal matrix with elements $\epsilon_i^{\frac{1}{2}}$. Then D is replaced by a diagonal matrix whose elements are all ≥ 0.

Corollary 2. *If T is a skew matrix with elements in $\mathfrak{F}_0(\sqrt{-1})$ there exists a unitary matrix such that $M^{-1}T\bar{M} = N'TN$ has the form* (4) *where $T_i = 0$ or is 2-rowed and skew.*

As in the symmetric case we may suppose that the matrices $T_i \neq 0$ are positive multiples of the matrix $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

Corollary 3. *If T is a unitary matrix with elements in $\mathfrak{F}_0(\sqrt{-1})$, there exists a unitary matrix M such that $M^{-1}T\bar{M} = N'TN$ has the form* (4) *where the T_i are unitary.*

In this case it is readily seen that we may normalize the T_i to have determinant $= 1$.

Now suppose that T and R are any two matrices such that $T\bar{T}' = T'\bar{T}$, $R\bar{R}' = R'\bar{R}$ and $T = M^{-1}R\bar{M}$ where M is unitary. Then $R\bar{R}$ and $T\bar{T} = M^{-1}R\bar{R}M$ are similar. We proceed to prove the converse. It has been

shown by Nakayama and by Haantjes [17] that if R and T are any two matrices with elements in $\mathfrak{F}_0(\sqrt{-1})$ such that rank $R\bar{R}\cdots\bar{R}^{(i)} =$ rank $T\bar{T}\cdots\bar{T}^{(i)}$ and $R\bar{R}$ and $T\bar{T}$ are similar, then there exists a matrix A such that $A^{-1}R\bar{A} = T$. Moreover in the present case it is clear from (4) that rank R $=$ rank $R\bar{R}\cdots\bar{R}^{(i)} =$ rank $T\bar{T}\cdots\bar{T}^{(i)} =$ rank T. Hence we may suppose that $A^{-1}R\bar{A} = T$ and also that R and T have the form (4). Thus R and T are matrices of the same normal a. l. t. $\mathbf{T}$. The irreducible matrices R_i and T_i correspond to two decompositions of R into irreducible invariant subspaces relative to T. Hence by the Jordan-Hölder theorem, we may suppose that $A_i^{-1}R_i\bar{A}_i = T_i$, $i = 1, 2, \cdots, l$. It therefore suffices to prove the following

LEMMA. *If R and T satisfy $R\bar{R}' = R'\bar{R}$, $T\bar{T}' = T'\bar{T}$ and these matrices belong to the same irreducible normal a. l. t., then there exists a unitary matrix M such that $M^{-1}R\bar{M} = T$.*

We have seen that $A^{-1}R\bar{A} = T$ and T and R have the form βU and γV where U and V are unitary and $\beta, \gamma \geqq 0$. The case $\beta = \gamma = 0$ is trivial. If $\beta \neq 0$ we obtain $A^{-1}V\bar{V}A = (\beta\gamma^{-1})^2U\bar{U}$. Since the roots of the unitary matrices $U\bar{U}$ and $V\bar{V}$ have absolute value 1, this implies $\beta^2 = \gamma^2$ and $\beta = \gamma$. Thus we may suppose that R and T are unitary. Then $T = \bar{A}'R(A')^{-1}$ and $BR = R\bar{B}$ if $B = A\bar{A}'$. As the author has shown [18] the matrices X satisfying the equation $XR = R\bar{X}$ form a division algebra over $\mathfrak{F}_0$. On the other hand B is hermitian and positive definite and hence it satisfies a quadratic equation whose roots are real and positive in $\mathfrak{F}_0$. Hence $B = \delta 1$, $\delta > 0$ and $A = \delta^{\frac{1}{2}}M$ where M is unitary. Then $T = M^{-1}R\bar{M}$.

THEOREM 11. *A necessary and sufficient condition that two matrices R and T with elements in $\mathfrak{F}_0(\sqrt{-1})$ such that $R\bar{R}' = R'\bar{R}$, $T\bar{T}' = T'\bar{T}$ be related by a unitary matrix M in the manner $M^{-1}R\bar{M} = N'RN = T\,(N = \bar{M})$ is that $R\bar{R}$ and $T\bar{T}$ be similar.*

8. We suppose in this section that $\mathfrak{F}$ is Hamilton's quaterion algebra over a real closed field $\mathfrak{F}_0$. Besides the well-known i. a. a.

$$\alpha = \alpha_0 + i\alpha_1 + j\alpha_2 + k\alpha_3 \rightarrow \bar{\alpha} = \alpha_0 - i\alpha_1 - j\alpha_2 - k\alpha_3$$

we have the i. a. a.'s $\alpha \rightarrow \alpha^V = \nu^{-1}\bar{\alpha}\nu$ where $\nu = -\nu$.[19] However if $f = (x, y)$

---

[17] Nakayama, "Über die Klassifikation halblinearer Transformationen," *Proc. Phys.-Math. Soc. Japan*, vol. 19 (1937); Haantjes, "Halblineare transformationen," *Mathematische Annalen*, Bd. 114 (1937), pp. 292-304.

[18] *Loc. cit.* in 6, p. 503.

[19] There are the only i. a. a.'s in $\mathfrak{F}$ leaving the elements of $\mathfrak{F}_0$ unaltered. See, for example, Albert, "Involutorial simple algebras and real Riemann matrices," *Annals of Mathematics*, vol. 36 (1935), p. 897.

is a bilinear form with the i. a. a. V, then the condition $(x\alpha, y) = \nu^{-1}\bar{\alpha}\nu(x, y)$ implies that $\nu(x\alpha, y) = \bar{\alpha}\nu(x, y)$ and hence νf is a bilinear form with the usual i. a. a. $\alpha \to \bar{\alpha}$. It is readily seen that f is hermitian or skew if and only if νf is respectively skew or hermitian. Since the adjoints of an l. t. defined relative to f and νf are equal we shall consider only the i. a. a. $\alpha \to \bar{\alpha}$.

We shall show next that if f is totally regular and dim $R > 1$ then f can not be skew. For suppose u and v are orthogonal and $(u, u) = \gamma$, $(v, v) = \delta$ where $\bar{\gamma} = -\gamma$, $\bar{\delta} = -\delta$. It can be shown that $-\gamma$ and δ are cogredient in the sense that there is an α in $\mathfrak{F}$ such that $\delta = -\bar{\alpha}\gamma\alpha$.[20] Then $(u\alpha + v, u\alpha + v) = 0$ contrary to the total regularity. Thus f is hermitian and as in the complex case we may suppose that it is positive definite.

It follows that $\mathfrak{R}$ has a *unitary* basis of vectors $u_1, u_2, \cdots, u_n$ such that $(u_i, u_j) = \delta_{ij}$. Any other unitary basis is obtained from the u's by transformation with a unitary matrix. The l. t. $\boldsymbol{T}$ is normal if and only if its matrix T relative to the u's satisfies $T\bar{T}' = \bar{T}'T$.

If $\phi(t) \in \mathfrak{F}[t]$, $\phi^*(t) = \phi(t)\bar{\phi}(t) \in \mathfrak{F}_0[t]$ the centrum of $\mathfrak{F}[t]$. Evidently $\phi^*(t)$ can be decomposed into linear factors in $\mathfrak{F}[t]$ and hence by the factorization theorem[21] $\phi(t)$ has linear factors. Thus the only irreducible polynomials in $\mathfrak{F}[t]$ are linear and hence the irreducible subspaces of an l. t. are 1-dimensional.

Suppose $\boldsymbol{T}$ is normal and $\mathfrak{S}$ is irreducible in $\mathfrak{L}(\boldsymbol{T})$. If $u \neq 0$ is in $\mathfrak{S}$, $u\boldsymbol{T} = u\beta$ and

$$(u\bar{\beta}, u) = \beta(u, u) = (u, u)\beta = (u, u\beta) = (u, u\boldsymbol{T}) = (u\boldsymbol{T}^*, u)$$

since $(u, u) \in \mathfrak{F}_0$. Hence $(u(\bar{\beta} - \boldsymbol{T}^*), u) = 0$ and

$$\begin{aligned}(u(\bar{\beta} - \boldsymbol{T}^*), u(\bar{\beta} - \boldsymbol{T}^*)) &= (u(\bar{\beta} - \boldsymbol{T}^*), u\bar{\beta}) - (u(\bar{\beta} - \boldsymbol{T}^*), u\boldsymbol{T}^*) \\ &= -(u(\bar{\beta} - \boldsymbol{T}^*), u\boldsymbol{T}^*) \\ &= -(u\boldsymbol{T}(\bar{\beta} - \boldsymbol{T}^*), u) \\ &= -\bar{\beta}(u(\bar{\beta} - \boldsymbol{T}^*), u) = 0.\end{aligned}$$

Hence $u\boldsymbol{T}^* = u\bar{\beta}$, i. e., $\mathfrak{S}$ is invariant relative to $\boldsymbol{T}^*$.

THEOREM 12. *If $\boldsymbol{T}$ is a normal l. t. in $\mathfrak{R}$ over $\mathfrak{F}$ where $\mathfrak{F}$ is a quaternion algebra over a real closed field, then $\boldsymbol{T}$ is orthogonally completely reducible.*

As before, we obtain

---

[20] Jacobson, "Simple Lie algebras of characteristic zero," *Duke Mathematical Journal*, vol. 4 (1938), p. 546.

[21] Ore, "Non-commutative polynomials," *Annals of Mathematics*, vol. 34 (1933), p. 494.

THEOREM 13. *If T is normal matrix $(T\bar{T}' = \bar{T}'T)$ with elements in $\mathfrak{F}$, there exists a unitary matrix M such that $M^{-1}TM = \bar{M}'TM$ is diagonal.*[22]

In the special cases $\boldsymbol{T}^* = \boldsymbol{T}$, $\boldsymbol{T}^* = -\boldsymbol{T}$ and $\boldsymbol{T}\boldsymbol{T}^* = 1$ the diagonal elements β_i of T satisfy the conditions $\bar{\beta}_i = \beta_i \in \mathfrak{F}_0$, $\bar{\beta}_i = -\beta_i$ and $\beta_i\bar{\beta}_i = 1$ respectively.

9. The above results may be interpreted also in projective geometry. We define the projective space $\mathfrak{P}$ of $(n-1)$-dimensions over $\mathfrak{F}$ as the set of subspace of the n-dimensional vector space $\mathfrak{R}$ over $\mathfrak{F}$. The points of $\mathfrak{P}$ are the rays $x\alpha$, $x \neq 0$ and fixed and α variable. The correspondence π: $\mathfrak{S} \to \mathfrak{S}' \equiv \mathfrak{S}\pi$ determined by a totally regular hermitian or skew-hermitian form f is called an *elliptic polarity*.[23]

It is known that any $(1-1)$ mapping τ of the elements of (the subspaces of $\mathfrak{R}$) which preserves incidences is determined by a non-singular s. l. t. $\boldsymbol{T}$.[24] τ will be called a semi-collination. Two s. l. t.'s $\boldsymbol{T}_1$ and $\boldsymbol{T}_2$ define the same τ if and only if $\boldsymbol{T}_1 = \boldsymbol{T}_2\rho$, $\rho \neq 0$ in $\mathfrak{F}$. τ is a collineation if the automorphism of $\boldsymbol{T}$ is inner; hence, if and only if $\boldsymbol{T}$ may be chosen as an l. t.

If τ is a semi-collineation, then so is $\tau' = \pi\tau\pi = \pi^{-1}\tau\pi$. Since $(x, y) = 0$ if and only if $(x(\boldsymbol{T}^*)^{-1}, y\boldsymbol{T}) = 0$, we see that if $\mathfrak{S}$ is a subspace and $\mathfrak{S}\pi$ its polar then $\mathfrak{S}(\boldsymbol{T}^*)^{-1}$ is the polar of $\mathfrak{S}\pi\tau$. Hence $\mathfrak{S}(\boldsymbol{T}^*)^{-1} = \mathfrak{S}\pi\tau\pi$. Thus the semi-collineation τ' is determined by $(\boldsymbol{T}^*)^{-1}$. We shall call τ normal if $\tau\tau' = \tau'\tau$. The condition on $\boldsymbol{T}$ is $\boldsymbol{T}\boldsymbol{T}^* = \boldsymbol{T}^*\boldsymbol{T}\mu$, $\mu \in \mathfrak{F}$. Notable special cases are given by the condition $\tau' = \tau$ and $\tau' = \tau^{-1}$.

It is known that if $\mathfrak{P}$ satisfies certain topological conditions, then $\mathfrak{F}$ must be either the field of real numbers, the field of complex numbers or the quasi-field of real quaternions.[25] We shall now discuss these cases separately.

(1). Suppose $\mathfrak{F}$ is the field of real numbers. The only automorphism or anti-automorphism of $\mathfrak{F}$ is the identity. It follows as in § 6 that if π is an elliptic polarity, the corresponding f may be assumed positive definite. Every semi-collineation τ is a collineation.

Suppose τ is normal. The condition $\tau'\tau = \tau\tau'$ is equivalent to $\boldsymbol{T}^*\boldsymbol{T}$

---

[22] Cf. Teichmüller, "Operatoren im Wachsschen Raum," *Crelle*, Bd. 174 (1935), p. 111.

[23] Veblen and Young, *Projective Geometry II*, p. 218. Cf. also Cartan, *La géometrie projective complexe*, p. 139. Cartan calls the correspondences determined by forms whose anti-automorphisms are different from the identity *anti-polarities*. From the present point of view it does not seem worth while to make this distinction.

[24] Cf. Brauer, "A characterization of null systems in projective space," *Bulletin of the American Mathematical Society*, vol. 42 (1936), pp. 247-254.

[25] Veblen and Young, *Projective Geometry II*, chap. 1, and Kolmogoroff, "Zur Begründung der projektiven Geometrie," *Annals of Mathematics*, vol. 33 (1932), pp. 175-176.

$= \boldsymbol{T}\boldsymbol{T}^*\mu$, $\mu \neq 0$ in $\mathfrak{F}$. Hence $TT' = T'T\mu$ if T is the matrix of $\boldsymbol{T}$ relative to a suitable basis. If $T = (\tau_{ij})$, $\operatorname{tr} TT' = \Sigma\tau_{ij}{}^2 \neq 0$ and since $\operatorname{tr} TT' = \operatorname{tr} T'T$, we obtain $\mu = 1$ and hence $\boldsymbol{T}$ is a normal l. t. $\tau' = \tau$ if and only if $\boldsymbol{T}^*\boldsymbol{T} = 1\rho$, $\rho > 0$. If we replace $\boldsymbol{T}$ by $\boldsymbol{T}\rho^{-\frac{1}{2}}$, we see that $\boldsymbol{T}$ can be taken as a unitary (orthogonal) l. t. On the other hand $\tau' = \tau^{-1}$ if and only if $\boldsymbol{T}^* = \boldsymbol{T}\mu$ and since $\boldsymbol{T}^{**} = \boldsymbol{T}$, we obtain $\mu^2 = 1$ and $\boldsymbol{T}^* = \pm \boldsymbol{T}$.

(2). $\mathfrak{F}$ is the field of complex numbers. In this case we restrict ourselves to continuous polarities and semi-collineations. The corresponding anti-automorphism or automorphism will be continuous. Hence we have just two types, the identity and the mapping $\alpha \to \bar{\alpha}$. A bilinear form with the identity as its anti-automorphism can not be totally regular. It follows (§ 7) that any elliptic polarity is determined by a positive definite hermitian form.

There are two types of continuous semi-collineations: the collineations and the semi-collineations with the automorphism $\alpha \to \bar{\alpha}$. The latter are called *anti-collineations.* If τ is a normal collineation then $\boldsymbol{T}\boldsymbol{T}^* = \boldsymbol{T}^*\boldsymbol{T}\mu$ and conversely. Hence $T\bar{T}' = \bar{T}'T\mu$ and since $\operatorname{tr} T\bar{T}' = \Sigma|\tau_{ij}|^2 \neq 0$ we obtain $\mu = 1$ and hence $\boldsymbol{T}$ is normal. The condition $\tau' = \tau$ means that $\boldsymbol{T}\boldsymbol{T}^* = 1\rho$ and as before $\boldsymbol{T}$ may be taken unitary. $\tau' = \tau^{-1}$ is equivalent to $\boldsymbol{T}^* = \boldsymbol{T}\rho$ and hence $\boldsymbol{T}^{**} = \boldsymbol{T}^*\bar{\rho}\rho = \boldsymbol{T}\bar{\rho}\rho = \boldsymbol{T}$, $\bar{\rho}\rho = 1$. If we replace $\boldsymbol{T}$ by $\boldsymbol{T}\sigma$ where $\rho = \bar{\sigma}^{-1}\sigma$ we see that τ is determined by a self-adjoint l. t.

If τ is a normal anti-collineation, $\boldsymbol{T}\boldsymbol{T}^* = \boldsymbol{T}^*\boldsymbol{T}\mu$. The matrices of these l. t. are respectively $T\bar{T}'$ and $T'\bar{T}\mu$. It follows again that $\mu = 1$ and $\boldsymbol{T}$ is a normal a. l. t. and conversely. $\tau' = \tau$ if and only if $\boldsymbol{T}$ can be taken as a unitary a. l. t. and $\tau' = \tau^{-1}$ if and only if $\boldsymbol{T}$ is either self-adjoint or skew.

(3). $\mathfrak{F}$ is the field of real quaternions. Any anti-automorphism or automorphism of $\mathfrak{F}$ maps the center $\mathfrak{F}_0$ into itself and since $\mathfrak{F}_0$ is the field of real numbers, the elements of $\mathfrak{F}_0$ are left invariant. It follows that the antimorphisms of $\mathfrak{F}_0$ are $\alpha \to \bar{\alpha}$ and $\alpha \to \nu^{-1}\bar{\alpha}\nu$, $\bar{\nu} = -\nu$ and the automorphisms are all inner. Hence as we saw in § 8, the elliptic polarities in $\mathfrak{P}$ are determined by positive definite hermitian forms. The semi-collineations in $\mathfrak{P}$ are all collineations. τ is normal if and only if the corresponding l. t. is normal; $\tau' = \tau$ if and only if T can be chosen unitary; $\tau' = \tau^{-1}$ if and only if $\boldsymbol{T}$ is self-adjoint or skew.

The results of § 6-8 may be translated to the present situation. For example we have the following theorem:

Let $\mathfrak{P}$ be a continuous projective space in the above sense, π a continuous elliptic polarity and τ a continuous normal collineation or anti-collineation in $\mathfrak{P}$. Then if $\mathfrak{S}$ is a hyperplane invariant under τ, its polar plane $\mathfrak{S}\pi$ is also invariant under τ.

University of North Carolina.

FOUNDATIONS OF AN ABSTRACT THEORY OF ABELIAN FUNCTIONS.*

By O. F. G. Schilling.[1]

It is a well-known fact that the classical theory of algebraic curves can be generalized to fields of algebraic functions of one variable over an arbitrary field of coefficients. Two topics are of particular interest from the viewpoint of modern algebra: The generalization of Riemann-Roch's theorem and related questions and the application of the algebraico-arithmetic theory of function fields to the theory of higher congruences. Using the arithmetic theory of the Riemann surface as developed by Hensel and Landsberg it is relatively easy to prove the generalized theorem of Riemann-Roch. However, with respect to the applications to the theory of higher congruences—in particular the applications to Artin's formulation [2,3] of the equivalent of Riemann's hypothesis concerning the zeta function belonging to a field of algebraic functions of one variable over a finite Galois field—unforeseen difficulties arose. Hasse succeeded to prove Artin's conjecture for generalized elliptic fields.[4] Typical for Hasse's approach is the investigation of the relationship between the unramified abelian extensions of the elliptic field and its isomorphic subfields. In order to find a proof of Artin's conjecture for non-elliptic fields, it appears to be advisable that one should generalize the algebraic results of Hasse. As a consequence of Riemann-Roch's theorem one surely cannot develop the analogue of Hasse's algebraic theory in the given function field of genus $p > 1$ proper. However, we know from the classical theory of abelian functions of p variables that the natural generalization of the elliptic case is found in the field of abelian functions related to the given Riemann surface of genus $p > 1$. Since one cannot develop the topological theory of the Riemann surface for function fields over abstract fields of coefficients, the function theoretic aspects of the abelian functions, i. e. their $2p$-fold periodicity, have to be discarded. Never-

* Received September 19, 1938.

[1] Johnston scholar at the Johns Hopkins University for the year 1938-1939.

[2] E. Artin, "Quadratische Körper im Gebiete der höheren Kongruenzen," II, *Mathematische Zeitschrift*, vol. 19 (1924).

[3] H. Hasse, "Über die Kongruenzzetafunktionen," *Sitzungsber. der Preuss. Akad. der Wissenschaften, Phys.-Math. Klasse* (1934).

[4] H. Hasse, "Zur Theorie der abstrakten elliptischen Funktionenkörper," I-III, *Crelle*, vol. 175 (1936).

theless, a careful study of Weierstrass' solution of the inversion problem of abelian integrals leads to a natural way out of this dilemma. Moreover, G. Castelnuovo [5] developed in a paper concerning complete linear series on a curve some essential facts concerning the fields of abelian functions belonging to a complex curve. Castelnuovo's proofs are algebraico-geometric. We want to present in this paper an elaboration of all these ideas by means of modern algebra. We want to point out that v. d. Waerden's notion of generic point on an algebraic variety proved to be a rather helpful tool.[6] It is then possible to define the abstract field of abelian functions as the p-fold symmetric product of the given function field of genus p. There will be no restrictions arising from the characteristic of the underlying field of coefficients. We shall show that the group of all birational transformations of the field of abelian functions contains the reflection and a subgroup which is isomorphic with the group of all divisor classes of degree 0. Moreover we shall develop the theory of natural multiplications. Finally, we indicate the connections with the classical theory, observing that our theory represents the straightforward generalization of the latter.

We hope to be able to present in other papers an algebraic theory of the complex multiplications and related topics.

1. The field of algebraic functions of one variable. Let $K = \{a\}$ be a field of algebraic functions of one variable whose field of coefficients is an arbitrary algebraically closed field k of characteristic χ. It is a well-known fact that K has a separable generation $k(x, y) = K$, i. e. y is a separable quantity over the field $k(x)$.

A prime divisor or valuation $\mathfrak{p}$ of K is given by an ordering function $v_\mathfrak{p}$ on K whose values are integers. Moreover, the function $v_\mathfrak{p}$ has the properties

$$\begin{aligned} v_\mathfrak{p}(ab) &= v_\mathfrak{p}(a) + v_\mathfrak{p}(b), \\ v_\mathfrak{p}(a+b) &\geqq \min(v_\mathfrak{p}(a), v_\mathfrak{p}(b)), \\ v_\mathfrak{p}(c) &= 0 \text{ if } c \in k, \text{ and} \\ v_\mathfrak{p}(0) &= \infty. \end{aligned}$$

To every valuation $\mathfrak{p}$ we can associate a prime ideal $\bar{\mathfrak{p}}$ of a suitably chosen integrally closed ring $\mathfrak{O}_z$ of K. Namely, take a non-constant function $z \in K$ such that $v_\mathfrak{p}(z) \geqq 0$ and consider the ring $\mathfrak{O}_z$ of all integral functions of K over $k[z]$. Then

$$\bar{\mathfrak{p}} = \mathfrak{O}_z \cap \{v\ (a) \geqq 0,\ a \in K\}.$$

[5] G. Castelnuovo, *Le correspondence univoche tra gruppi di p punti sopra una curve di genere p. Lomb. Ist. Rend.*, vol. 25, ser. 2 (1892).

[6] B. L. van der Waerden, "Zur algebraischen Geometrie XIII," Vereinfachte Grundlagen. *Mathematische Annalen*, vol. 115 (1938).

Conversely, the prime ideals $\bar{\mathfrak{p}}$ of an integrally closed ring $\mathfrak{O}$ of K give rise to almost all prime divisors $\mathfrak{p}$ of K, only a finite number of valuations being excluded. The given ring $\mathfrak{O}$ can be considered as the ring of all integral functions in K with respect to a ring of polynomials $k[z]$ where $z \in \mathfrak{O}$. Thus, we can speak of the valuations $\mathfrak{p}$ corresponding to the prime ideals $\mathfrak{p}$ of $\mathfrak{O}$ as the finite valuations with respect to z. The prime divisors which cannot be determined relative to $\mathfrak{O}$ are the prime divisors of K which are poles of the function z. They correspond to prime ideals of the ring $\mathfrak{O}_{z^{-1}}$ over $k[z^{-1}]$.

The field K can be considered as the field of all rational functions on a curve C without singularities which is imbedded in the 3-dimensional projective space $P_3(k) = k[X_0, X_1, X_2, X_3]$ over the algebraically closed field k.[7] The points $\bar{\mathfrak{p}} = \bar{\mathfrak{p}}(a_0, a_1, a_2, a_3)$ of C are then in one to one correspondence with the prime divisors of K. The curve C is then a projective normal variety.

The residues x_1, x_2, x_3 of $X_1X_0^{-1}$, $X_2X_0^{-1}$, $X_3X_0^{-1}$ modulo the defining prime ideal $\mathfrak{m}(C) = (f_1(X_0, X_1, X_2, X_3), \cdots, f_m(X_0, X_1, X_2, X_3))$ determine an integrally closed ring $\mathfrak{O} = k[x_1, x_2, x_3]$ of K. The ring $\mathfrak{O}$ resp. the base x_1, x_2, x_3, gives rise to a normal affine curve $C(\mathfrak{O})$. The substratum of functions $(x_1, x_2, x_3) = [x]$ is called a generic point of $C(\mathfrak{O})$. All special points on C resp. on $C(\mathfrak{O})$ are obtained by specializing the respective generic points. For example, $(X_0, X_1, X_2, X_3) \rightarrow (a_0, a_1, a_2, a_3) \neq (0, 0, 0, 0)$ where $a_i \in k$ and $f_\nu(a_0, a_1, a_2, a_3) = 0$, $\nu = 1, \cdots, m$.

For later considerations it will be convenient to consider the generic point $[x]$ of $C(\mathfrak{O})$ as a point of a suitably chosen curve. Suppose that $[\bar{x}] = [\bar{x}_1, \bar{x}_2, \bar{x}_3]$ is a set of elements which satisfies the relations between x_1, x_2, x_3 such that the field $\bar{K} = k(\bar{x}_1, \bar{x}_2, \bar{x}_3)$ is abstractly isomorphic with K. $K \cap \bar{K} = k$. Next extend the field of coefficients k of $\bar{K}$ to the field K, i. e. consider the ring

$$\bar{K}K = K(\bar{x}_1, \bar{x}_2, \bar{x}_3).$$

This ring is a function field of one variable over K as field of coefficients. Let L be the algebraically closed field of K. Then also $\bar{K}L$ is a field. This follows from a general theorem concerning the decomposition of the defining prime ideal of relations of $\bar{K}$ when the original algebraically closed field of coefficients is extended to an arbitrarily relatively transcendental field.

Obviously the ring $\bar{\mathfrak{O}}L = L[\bar{x}_1, \bar{x}_2, \bar{x}_3]$ is also integrally closed in $\bar{K}L$. Since $\bar{x}_1, \bar{x}_2, \bar{x}_3$ generate the ring $\bar{\mathfrak{O}} \cong \mathfrak{O}$ it follows that $(\bar{x}_1, - x_1, \bar{x}_2 - x_2,$

---

[7] H. T. Muhly and O. Zariski, "The resolution of the singularities of an algebraic curve" to appear in the *American Journal of Mathematics*, and a paper of O. Zariski on algebraic varieties.

$\bar{x}_3 - x_3)$ is a prime ideal $\bar{\mathfrak{P}}$ of $\bar{\mathfrak{O}}L$. Let $\mathfrak{P}$ be the corresponding prime divisor of $\bar{K}L$. Then

$$\bar{x}_i \equiv x_i \pmod{\mathfrak{P}}, \qquad (i = 1, 2, 3).$$

We shall say that we have represented the general point $[x]$ of $C(\mathfrak{O})$ by a point of the curve $C(\bar{\mathfrak{O}}L)$.

Each divisor $\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{p}_i^{\alpha_i}$, α_i integers, determines uniquely a class of divisors $\mathfrak{A} = \mathfrak{a}(a)$ where (a) runs over the totality of all divisors belonging to elements a of K. The common degree $\deg \mathfrak{a} = \sum_{i=1}^{s} \alpha_i$ of all divisors $\mathfrak{a}$ in a class $\mathfrak{A}$ is called the degree $\deg \mathfrak{A}$ of the class $\mathfrak{A}$.

If the degree of a class $\mathfrak{A}$ is greater than 0 then $\mathfrak{A}$ contains integral divisors $\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{p}_i^{\alpha_i}$, $\alpha_i > 0$. All integral divisors $\mathfrak{a}$ of such a class form a finite k-module. The rank $\dim \mathfrak{A}$ of this module is called the dimension of the class. The explicit determination of $\dim \mathfrak{A}$ is given by the theorem of Riemann-Roch

$$\dim \mathfrak{A} = \dim \mathfrak{A}\mathfrak{K}^{-1} + \deg \mathfrak{A} - p + 1.$$

The class $\mathfrak{K}$ is the so-called canonical class of K whose integral divisors are the differentials of first kind. We have

$$\deg \mathfrak{K} = 2p - 2, \qquad \dim \mathfrak{K} = p \geqq 0$$

where p is the genus of the field K.[8]

The divisor classes $\mathfrak{A}$ of positive degree correspond to the complete linear series of the classical theory. It can be proved that the integral divisors $\mathfrak{a}$ of $\mathfrak{A}$ correspond to the hypersurfaces of a suitable projective space which cut out the individual groups of the linear series. In particular, we can interpret the coördinates of a curve in projective space as the divisors of a basic set for the k-module of integral divisors of a well-defined divisor class of K.

We shall pay special attention to two types of classes. Firstly, the classes of degree p which we shall denote by $\mathfrak{A}_p$. It can be proved as a consequence of the theorem of Riemann-Roch that there exist infinitely many classes $\mathfrak{A}_p$ for which $\dim \mathfrak{A}_p = 1$. Moreover, infinitely many such classes $\mathfrak{A}_p$ contain exactly one integral divisor $\mathfrak{r}_1 \cdots \mathfrak{r}_p$ where the $\mathfrak{r}_i$ are distinct prime divisors of K.[9] We write $\mathfrak{r}_1 \cdots \mathfrak{r}_p = \mathfrak{R}_p$.

---

[8] F. K. Schmidt, "Zur arithmetischen Theorie der algebraischen Funktionen," I, *Mathematische Zeitschrift*, vol. 41 (1936).

[9] E. Witt and H. Hasse, "Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Characteristik p," *Monatshefte für Mathematik und Physik*, vol. 43 (1936).

Secondly, the group of all divisor classes contains the subgroup $\boldsymbol{D}$ which consists of all classes $\mathfrak{C}$ of degree 0. Since the degree of a class is an additive function of the arguments it follows that each class $\mathfrak{C}$ determines uniquely a class $\mathfrak{A}_p$ with respect to fixed reference class $\mathfrak{R}_p$. Namely,

$$\mathfrak{A}_p = \mathfrak{C}\mathfrak{R}_p, \text{ or}$$
$$\mathfrak{C} = \mathfrak{A}_p\mathfrak{R}_p^{-1}.$$

A class $\mathfrak{A}_p$ whose dimension is greater than 1 shall be called an exceptional class.

2. The field of abelian functions. Let $K = k(x_1, x_2, x_3)$ be a field of algebraic functions of one variable such that x_1, x_2, x_3 span up an integrally closed ring $\mathfrak{O} = k[x_1, x_2, x_3]$. Suppose now that

$$K^{(i)} = k(x_1^{(i)}, x_2^{(i)}, x_3^{(i)}) = K * I^{(i)}$$

are p fields which are abstractly isomorphic with K and which are algebraically independent over k. Then $k(x_1^{(1)}, \cdots, x_1^{(p)})$ is a field of rational functions of p variables over k. Consequently, the join of the fields $K^{(1)}, \cdots, K^{(p)}$ in the algebraically closed field of $k(x_1^{(1)}, \cdots, x_1^{(p)})$ is a field $\Delta_p(K) = K^{(1)} \times \cdots \times K^{(p)}$ of degree of transcendency p with respect to k. It is called the p-fold direct product of K by itself. The field $\Delta_p(K)$ contains the order $\mathfrak{O}^{(1)} \times \cdots \times \mathfrak{O}^{(p)} = \Delta_p(\mathfrak{O})$ where $\mathfrak{O}^{(i)} = \mathfrak{O} * I^{(i)}$.

Since $\Delta_p(\mathfrak{O})$ is spanned up by the functions $(x_1^{(1)}, x_2^{(1)}, x_3^{(1)}, \cdots, x_1^{(p)}, x_2^{(p)}, x_3^{(p)}) = [x^{(1)}, \cdots, x^{(p)}]$ we see that $[x^{(1)}, \cdots, x^{(p)}]$ is the generic point $\mathfrak{P}'$ of a p-dimensional algebraic variety $V'(\mathfrak{O})$. The variety $V'(\mathfrak{O})$ is imbedded in the $3p$-dimensional affine space over k. Each point $\mathfrak{P}'_0$ of $V'(\mathfrak{O})$ is obtained by admissible specializations of $\mathfrak{P}'$.

This affine variety $V'(\mathfrak{O})$ can be obtained from the direct product $\Delta_p(C)$ of a projective model C of K without singularities in the 3-dimensional space. The variety $\Delta_p(C)$ is imbedded in the p-fold direct product of the projective 3-space over k. Each point $\mathfrak{P}'_0$ of $\Delta_p(C)$ is obtained from a suitable generic point $\mathfrak{P}'$ of $\Delta_p(C)$ by an admissible specialization. Obviously a generic point $\mathfrak{P}'$ of $\Delta_p(C)$ is given as

$$[X^{(1)} \bmod \mathfrak{m}(C^{(1)}), \cdots, X^{(p)} \bmod \mathfrak{m}(C^{(p)})]$$

where $X^{(i)} = [X_0^{(i)}, X_1^{(i)}, X_2^{(i)}, X_3^{(i)}]$ denote the projective coördinates of the projective 3-space in which the curve $C^{(i)} = C * I^{(i)}$ with the defining relations $\mathfrak{m}(C^{(i)})$ is imbedded.

The points $\mathfrak{P}'_0$ of $\Delta_p(C)$ are related to the p-tuples $\mathfrak{p}_1, \cdots, \mathfrak{p}_p$ of prime

divisors of K. Let s be an arbitrary substitution $\binom{1,\cdots,p}{j_1,\cdots,j_p}$ of the symmetric group S_p of p objects. Suppose moreover that there are given p prime divisors $\mathfrak{p}_1,\cdots,\mathfrak{p}_p$ of K which can be represented by prime ideals $\bar{\mathfrak{p}}_1,\cdots,\bar{\mathfrak{p}}_p$ of $\mathfrak{O}$. Then let correspond to $\bar{\mathfrak{p}}_i$ the prime ideal $\bar{\mathfrak{p}}_i * I^{(j_i)}$ of the normal variety $C(\mathfrak{O}) * I^{(j_i)}$ where $I^{(j_1)},\cdots,I^{(j_p)}$ are obtained from the given $I^{(1)},\cdots,I^{(p)}$ by applying the permutation s. The greatest common divisor

$$(\bar{\mathfrak{p}}_1 * I^{(j_1)},\cdots,\bar{\mathfrak{p}}_p * I^{(j_p)}) \text{ in } \Delta_p(C(\mathfrak{O}))$$

is then a 0-dimensional prime ideal $\mathfrak{P}'_{0,s}(\mathfrak{p}_1,\cdots,\mathfrak{p}_p)$ of $\Delta_p(\mathfrak{O})$, i. e. a point of $\Delta_p(C(\mathfrak{O}))$. In order to obtain the points of $\Delta_p(C)$ we only have to change $\mathfrak{O}$. Thus, each p-tuple of prime divisors $\mathfrak{p}_1,\cdots,\mathfrak{p}_p$ of K gives rise to $p!$ points $\mathfrak{P}'_{0,s}(\mathfrak{p}_1,\cdots,\mathfrak{p}_p)$ on $\Delta_p(C)$.

Conversely, each point $\mathfrak{P}'_0$ on $\Delta_p(C)$ determines a p-tuple of prime divisors of K. Namely, the quantities $x_i^{(j)} = X_i^{(j)} \bmod \mathfrak{m}(C^{(j)})$ assume definite constant values $a_i^{(j)} = x_i^{(j)} \bmod \mathfrak{P}'_0$ at the point $\mathfrak{P}'_0$ since $\mathfrak{P}'_0$ is defined by a specialization of the generic point $\mathfrak{P}'$ of $\Delta_p(C)$. Now each set of values $(a_0^{(j)},\cdots,a_3^{(j)})$, $j=1,\cdots,p$, determines uniquely a point $(x_0^{(j)}-a_0^{(j)},\cdots,x_3^{(j)}-a_3^{(j)})$ of $C^{(j)}$. Hence a prime divisor $\mathfrak{p}^{(j)}$ of $K^{(j)}$. The inverse mappings $I^{(j)-1}$ for which $K^{(j)} * I^{(j)-1} = K$ determine p prime divisors $\mathfrak{p}_j$ of K. We let correspond to $\mathfrak{P}'_0$ the p-tuple $\mathfrak{p}_1,\cdots,\mathfrak{p}_p$. Thus the integral divisors of degree p are in $(1,p!)$ correspondence with the points on $\Delta_p(C)$.

It was already pointed out that a generic point (x_0,x_1,x_2,x_3) of the curve C can be considered as given by a prime divisor $\mathfrak{P}$ of the extended function field $\bar{K}L$. Similarly the generic point $(x_0^{(1)},\cdots,x_3^{(1)},\cdots,x_0^{(p)},\cdots,x_3^{(p)})$ of $\Delta_p(C)$ can be considered as an ordered p-tuple of prime divisors of a suitably chosen function field of one variable. Let $\bar{K}$ be an isomorphic map of K such that K and $\bar{K}$ are algebraically independent over k. Consider the extension $\bar{K}\Delta_p(K)$ of $\bar{K}$. To each component $K^{(i)}$ of $\Delta_p(K)$ there corresponds then a uniquely determined prime divisor $\mathfrak{P}_i$ of $\bar{K}\Delta_p(K)$. Using an affine model $C(\bar{\mathfrak{O}})$ of $\bar{K}$ we find that the prime divisors $P^{(i)}$ are given by prime ideals $\bar{\mathfrak{P}}_i$ of $\bar{\mathfrak{O}}\Delta_p(K)$. Namely,

$$\bar{\mathfrak{P}}_i = (\bar{x}_1 - x_1^{(i)},\cdots,\bar{x}_3 - x_3^{(i)}), \qquad (i=1,\cdots,p).$$

Thus the generic point $\mathfrak{P}'$ of $V'(\mathfrak{O})$ can be represented by a p-tuple of prime divisors of $\bar{K}\Delta_p(K)$. This construction is unique for we had to observe the fixed isomorphisms $I^{(i)}$. This construction obviously generalizes to the *representation of* $\Delta_p(K)$ by the variety $\Delta_p(C)$. In order to indicate this description of $\Delta_p(K)$ we shall write

$$\Delta_p(K) = K^{(1)} \times \cdots \times K^{(p)} = \mathfrak{P}_1 \times \cdots \times \mathfrak{P}_p.$$

Later on it will be convenient to denote $I^{(i)}$ by $I(\mathfrak{P}_i)$.

The field $\Delta_p(K)$ admits the symmetric group S_p as group of automorphisms. Namely, the structure of $\Delta_p(K)$ does not depend on the order of the fields $K^{(1)}, \cdots, K^{(p)}$. We shall define the automorphism which is related to $s = \binom{1, \cdots, p}{j_1, \cdots, j_p}$ as the permutation

$$([x^{(1)}], \cdots, [x^{(p)}]) \to ([x^{(j_1)}], \cdots, [x^{(j_p)}]).$$

The Galois theory implies then that all functions of $\Delta_p(K)$ which are left invariant by the $p!$ automorphisms constitute a subfield $A = \Sigma_p(K)$ of $\Delta_p(K)$.

We shall call A the field of abelian functions belonging to K, briefly the field of abelian functions.

The field of abelian functions has degree of transcendency p relative to k. It contains the p-fold symmetric product $\Sigma_p(\mathfrak{O}) = \Delta_p(\mathfrak{O}) \cap A$ of the integrally closed ring $\mathfrak{O}$ of K. The ring of integral functions $\Sigma_p(\mathfrak{O})$ gives rise to an algebraic variety $V_p(\mathfrak{O})$. This variety is according to construction a rational transform of $V'_p(\mathfrak{O})$. Similarly we obtain a symmetric product $\Sigma_p(C)$ which is a rational transform of $\Delta_p(C)$. To all the $p!$ points $\mathfrak{P}'_{0,s}$ on $\Delta_p(C)$ there corresponds one and the same point $\mathfrak{P}_0$ on $\Sigma_p(C)$. The associated prime ideal of $\mathfrak{P}_0$ (with regard to a suitably chosen integrally closed ring $\mathfrak{O}$) is the contracted ideal of the prime ideals corresponding to the $p!$ points $\mathfrak{P}'_{0,s}$. This process of contraction annihilates the $p!$ different arrangements of the prime divisors $\mathfrak{p}_1, \cdots, \mathfrak{p}_p$ which can be associated to all $\mathfrak{P}'_{0,s}$. Hence the points $\mathfrak{P}_0$ of $\Sigma_p(C)$ are in one to one correspondence with the unordered p-tuples of prime divisors in K. Thus we can associate to each point $\mathfrak{P}_0$ an integral divisor $\mathfrak{a}$ of degree p in K.

This relation extends immediately to the generic point $\mathfrak{P}$ of $\Sigma_p(C)$. We thus can represent the generic point $\mathfrak{P}$ of $\Sigma_p(C)$ by the product $\mathfrak{P}_1 \cdots \mathfrak{P}_p$ of the prime divisors $\mathfrak{P}_i$ which are defined in $\bar{K}\Delta_p(K)$. We express the field A symbolically as $\mathfrak{P}_1 \cdots \mathfrak{P}_p$. This notation refers to the construction of A the symmetric product of p general prime divisors of K, i. e. any set of generating functions of K. Since each point $\mathfrak{P}_0$ on $\Sigma_p(C)$ is obtained by specializing the generic point we see that $\mathfrak{P}_0$ is given by specializing the generic divisor $\mathfrak{P}_1 \cdots \mathfrak{P}_p$ of K to $\mathfrak{p}_1 \cdots \mathfrak{p}_p$, i. e. we perform a homomorphism of $\bar{K}L$ upon $\bar{K}$.

Now let $\mathfrak{A}_p$ be an arbitrary divisor class of degree p, then $\dim \mathfrak{A}_p = \delta(\mathfrak{A}_p) \geqq 1$. The integral divisors $\mathfrak{a}$ of $\mathfrak{A}_p$ can be considered as the points of a projective space over k whose dimension is equal to $\delta(\mathfrak{A}_p) - 1$. Consequently the totality of all integral divisors $\mathfrak{a}$ in $\mathfrak{A}_p$ gives rise to an algebraic irreducible

subvariety $\boldsymbol{M}(\mathfrak{A}_p, C)$ on $\boldsymbol{\Sigma}_p(C)$. The variety $\boldsymbol{M}(\mathfrak{A}_p, C)$ has dimension $\delta(\mathfrak{A}_p) - 1$. If $\delta(\mathfrak{A}_p) = 1$ then $\mathbf{M}(\mathfrak{A}_p, C)$ is a point $\mathfrak{P}_0$ on $\boldsymbol{\Sigma}_p(C)$ which is associated to the integral divisor $\mathfrak{a}$ of $\mathfrak{A}_p$. We denote the totality $\mathbf{M}(\mathfrak{A}_p, C)$ for variable classes $\mathfrak{A}_p$ by $\boldsymbol{W}(K)$.

3. Birational transformations of *A*. Let $\mathfrak{r}_1 \cdots \mathfrak{r}_p$ be an arbitrary divisor of degree p. We denote the divisor class which is uniquely determined by $\mathfrak{r}_1 \cdots \mathfrak{r}_p$ by $\mathfrak{R}_p$. Then $\dim \mathfrak{R}_p{}^3 = 2p + 1$ according to the theorem of Riemann-Roch. Consequently there exist $2p + 1$ linearly independent functions $\phi_0, \phi_1, \cdots, \phi_{2p}$ of K such that every function $\phi \in K$ which has at most the denominator $(\mathfrak{r}_1 \cdots \mathfrak{r}_p)^3$ can be expressed as $\sum_{i=0}^{2p} c_i \phi_i$ where $c_i \in k$.

Now let

$$\begin{aligned}
(x_1^{(1)},\ x_2^{(1)},\ x_3^{(1)}) &= [x^{(1)}] &&= [x] * I(\mathfrak{P}_1)\\
&\cdots\\
(x_1^{(p)},\ x_2^{(p)},\ x_3^{(p)}) &= [x^{(p)}] &&= [x] * I(\mathfrak{P}_p)\\
(x_1^{(p+1)}, x_2^{(p+1)}, x_3^{(p+1)}) &= [x^{(p+1)}] &&= [x] * I(\mathfrak{Q}_1)\\
&\cdots\\
(x_1^{(2p)},\ x_2^{(2p)},\ x_3^{(2p)}) &= [x^{(2p)}] &&= [x] * I(\mathfrak{Q}_p)
\end{aligned}$$

be the generating functions of $2p$ fields $K * I(\mathfrak{P}_1), \cdots, K * I(\mathfrak{P}_p)$, $K * I(\mathfrak{Q}_1), \cdots, K * I(\mathfrak{Q}_p)$ which are isomorphic with K and algebraically independent over k. Then their join J is a field of algebraic functions of $2p$ variables over k.

Let $\bar{N}$ be the algebraically closed field of J.

Next consider the function field $K\bar{N}$ which arises from K by extending the field of coefficients k to $\bar{N}$. The field $K\bar{N}$ has again genus p for it is generated by the elements (x_1, x_2, x_3) over $\bar{N}$. Moreover, the dimension of every class $\bar{\mathfrak{A}}_p$ of $K\bar{N}$ which contains a divisor $\mathfrak{a}_1, \cdots, \mathfrak{a}_p$ such that the residues of the $x_i \bmod \mathfrak{a}_j$ $(i = 1, \cdots, 3;\ j = 1, \cdots, p)$ lie in k is equal to the dimension of the class $\mathfrak{A}_p$ of K which is determined by $\mathfrak{a}_1 \cdots \mathfrak{a}_p$. Thus, a set of linearly independent integral divisors of $\mathfrak{A}_p$ constitutes also a base for the class $\bar{\mathfrak{A}}_p$.

The fields $K * I(\mathfrak{P}_1), \cdots, K * I(\mathfrak{P}_p)$, $K * I(\mathfrak{Q}_1), \cdots, K * I(\mathfrak{Q}_p)$ give rise to prime divisors $\mathfrak{P}_1, \cdots, \mathfrak{P}_p, \mathfrak{Q}_1, \cdots, \mathfrak{Q}_p$ of $K\bar{N}$. These prime divisors are of degree 1 relative to J.

Denote the divisor classes of $K\bar{N}$ which are generated by $\mathfrak{P}_1 \cdots \mathfrak{P}_p$ and $\mathfrak{Q}_1 \cdots \mathfrak{Q}_p$ by $\mathfrak{P}_p$ and $\mathfrak{O}_p$, respectively. Since $\mathfrak{P}_p$ and $\mathfrak{O}_p$ can be thought of as generic classes of degree p of K we have $\dim \mathfrak{P}_p = \dim \mathfrak{O}_p = 1$.

We propose to give an expression for the divisors $\mathfrak{s}_1, \cdots, \mathfrak{s}_p$ of $K\bar{N}$ for which

$$(\mathfrak{P}_p\mathfrak{R}_p^{-1})(\mathfrak{Q}_p\mathfrak{R}_p^{-1})(\mathfrak{S}_p\mathfrak{R}_p^{-1}) \approx 1.$$

Since all divisor classes of degree 0 in $K\bar{N}$ form an abelian group, the class $\mathfrak{S}_p\mathfrak{R}_p^{-1}$ is uniquely determined by our equation. It has to be proved that $\mathfrak{S}_p = \mathfrak{s}_1 \cdots \mathfrak{s}_p$ where the $\mathfrak{s}_i$ are mutually distinct prime divisors of degree 1 relative to J.

To determine $\mathfrak{s}_1, \cdots, \mathfrak{s}_p$ it suffices to find a function Φ of $K\bar{N}$ which has the divisor $(\mathfrak{r}_1 \cdots \mathfrak{r}_p)^3$ as denominator and the divisor $\prod_{i=1}^{p} \mathfrak{P}_i \prod_{i=1}^{p} \mathfrak{Q}_i$ as numerator.[10] According to the theorem of Riemann-Roch and the preceding remarks, this function $\bar{\Phi}$ must have the form

$$\bar{\Phi} = \sum_{i=0}^{2p} \bar{c}_i \Phi_i$$

where the coefficients $\bar{c}_i$ are taken from $\bar{N}$. This representation takes care of the assigned poles. Let $\Phi_i * \mathfrak{P}_j$, $\Phi_i * \mathfrak{Q}_j$—$i = 0, 1, \cdots, 2p$; $j = 1, \cdots, p$— be the residues of the functions Φ_i at the prime divisors $\mathfrak{P}_j$, Φ_i. The elements $\Phi_i * \mathfrak{P}_j$, $\Phi_i * \mathfrak{Q}_j$ lie in $\bar{N}$. Namely, according to construction, a function Φ_i has none of the prime divisors $\mathfrak{P}_j$ or $\mathfrak{Q}_j$ as pole.

Moreover, the residues $\Phi_i * \mathfrak{P}_j$, $\Phi_i * \mathfrak{Q}_j$ are different from 0 since Φ_i are functions of K. As such they are uniquely (to within multiplicative factors in k) determined by their divisor decomposition in K. Thus, the prime divisors $\mathfrak{P}_j$, $\mathfrak{Q}_j$ are not zeros of the Φ_i. To be precise, the residues $\Phi_i * \mathfrak{P}_j$, $\Phi_i * \mathfrak{Q}_j$ lie already in J for $\mathfrak{P}_j$, $\mathfrak{Q}_j$ are supposed to be prime divisors of degree 1 with respect to J.

Next, the condition that $\bar{\Phi}$ have the numerator $\prod_{i=1}^{p} \mathfrak{P}_i \prod_{i=1}^{p} \mathfrak{Q}_i$ can be expressed by means of a determinant. We get

$$\bar{\Phi} = \begin{vmatrix} \Phi_0 & \Phi_1 & \cdots & \Phi_{2p} \\ \Phi_0 * \mathfrak{P}_1 & \Phi_1 * \mathfrak{P}_1 & \cdots & \Phi_{2p} * \mathfrak{P}_1 \\ \vdots & \vdots & & \vdots \\ \Phi_0 * \mathfrak{P}_p & \Phi_1 * \mathfrak{P}_p & \cdots & \Phi_{2p} * \mathfrak{P}_p \\ \Phi_0 * \mathfrak{Q}_1 & \Phi_1 * \mathfrak{Q}_1 & \cdots & \Phi_{2p} * \mathfrak{Q}_1 \\ \vdots & \vdots & & \vdots \\ \Phi_0 * \mathfrak{Q}_p & \Phi_1 * \mathfrak{Q}_p & \cdots & \Phi_{2p} * \mathfrak{Q}_p \end{vmatrix}.$$

[10] K. W. S. Hensel and G. Landberg, *Theorie der algebraischen Funktionen einer Variabeln und ihre Anwendung auf algebraische Kurven und Abelsche Integrale,* p. 681 (1902).

It follows immediately that Φ is a rational function of $[x]$,

$$[x] * I(\mathfrak{P}_1), \cdots, [x] * I(\mathfrak{P}_p), \qquad [x] * I(\mathfrak{Q}_1), \cdots, [x] * I(\mathfrak{Q}_p).$$

Now we have to determine the remaining zeros of $\bar{\Phi}$. Without loss of generality we can suppose that K is a separable extension of $k(x_1) = k(x)$. Let N denote the norm taken from K to $k(x)$. Then $N(\bar{\Phi})$ is a polynomial in x. We know already $2p$ roots of $N(\Phi) = 0$, namely $x * \mathfrak{P}_j$, $x * \mathfrak{Q}_j$ where $j = 1, \cdots, p$. Consequently,

$$N(\Phi)[\prod_{j=1}^{p} (x - x * \mathfrak{P}_j) \prod_{j=1}^{p} (x - x * \mathfrak{Q}_j)]^{-1} = G_x(\Phi)$$
$$= x^p + \bar{\Psi}_1 x^{p-1} + \cdots + \bar{\Psi}_p$$

is a polynomial of degree p. The coefficients $\bar{\Psi}_\nu$ of $G_x(\bar{\Phi})$ are rational functions of $[x] * I(\mathfrak{P}_1) = [x * \mathfrak{P}_1], \cdots, [x] * I(\mathfrak{Q}_p) = [x * \mathfrak{Q}_p]$. The equation $G_x(\bar{\Phi}) = 0$ is a separable equation since the $\bar{\Psi}_\nu$ do not vanish identically. Let $\bar{y}_1, \cdots, \bar{y}_p$ be its roots. They determine uniquely prime divisors $\mathfrak{S}_1, \cdots, \mathfrak{S}_p$ of $K\bar{N}$ by means of the prime ideals $(x - \bar{y}_i)$ of $\bar{N}[x]$. Namely, the elements $\bar{y}_i$ of $\bar{N}$ are all distinct. The condition that exactly the p remaining zeros of $\bar{\Phi}$ have to be determined implies that each $\mathfrak{S}_i$ is uniquely determined by one of the prime ideals of the integrally closed ring $\bar{N}[x_1, x_2, x_3]$ whose intersections with $\bar{N}[x]$ are equal to $(x - \bar{y}_i)$.

Another implication of this determination of the prime divisors $\mathfrak{S}_i$ is the fact that $[x * \mathfrak{S}_i]$ are algebraic functions of $[x * \mathfrak{P}_1], \cdots, [x * \mathfrak{Q}_p]$. Moreover, $\dim \mathfrak{S}_p = 1$.

In order to prove that the $[x * \mathfrak{S}_i]$ are rational functions of the $[x * \mathfrak{P}_1]$, $\cdots, [x * \mathfrak{Q}_p]$ we apply the principle of specialization. Namely, there always exist specializations of the prime divisors $\mathfrak{P}_j$, $\mathfrak{Q}_j$ to prime divisors $\mathfrak{p}_j$, $\mathfrak{q}_j$ of K such that the determinant relation for $\bar{\Phi}$ does not become singular. From this fact one concludes that the respective solutions of $G_x(\bar{\Phi}) = 0$ give rise to distinct prime divisors $\mathfrak{s}_1, \cdots, \mathfrak{s}_p$ of K which are specializations of $\mathfrak{S}_1, \cdots, \mathfrak{S}_p$. Moreover, $\mathfrak{s}_1, \cdots, \mathfrak{s}_p$ determine a class of dimension 1. Consequently the functions $[x * \mathfrak{S}_i]$ are rational functions of $[x * \mathfrak{P}_i]$, $[x * Q_i]$ for otherwise we would obtain a contradiction to the existence of an infinity of unique solutions for the specialized prime divisors.

It is important to remark that $\mathfrak{s}_1, \cdots, \mathfrak{s}_p$ are still uniquely determined when $\mathfrak{P}_1, \cdots, \mathfrak{P}_p$ are generic and $\mathfrak{Q}_1, \cdots, \mathfrak{Q}_p$ specialized arbitrarily to $\mathfrak{q}_1, \cdots, \mathfrak{q}_p$. In particular, it follows that $\mathfrak{S}_p$ does not depend on the particular divisor $\mathfrak{q}_1 \cdots \mathfrak{q}_p$ which we chose to represent the class $\mathfrak{Q}_p$.

Applying the process of determining $\mathfrak{S}_p$ from $(\mathfrak{P}_p\mathfrak{R}_p^{-1})(\mathfrak{Q}_p\mathfrak{R}_p^{-1})(\mathfrak{S}_p\mathfrak{R}_p^{-1}) \approx 1$ twice it follows that the divisor $\mathcal{P}(-1)_1 \cdots \mathcal{P}(-1)_p$ which satisfies

$$(\mathfrak{P}_p\mathfrak{R}_p^{-1})(\mathfrak{P}(-1)_p\mathfrak{R}_p^{-1}) \approx 1$$

is uniquely determined. Using again the argument of specialization we find that the functions $[x * \mathcal{P}(-1)_i]$ lie in J and that they generate p fields $K(-1)_i \cong K$ which are algebraically independent over k.

Finally, the construction of $\mathcal{S}_1 \cdots \mathcal{S}_p$ and $\mathcal{P}(-1)_1 \cdots \mathcal{P}(-1)_p$ immediately implies that

(i) $\mathcal{S}_1, \cdots, \mathcal{S}_p$ depend symmetrically on $\mathcal{P}_1, \cdots, \mathcal{P}_p$ and $\mathcal{Q}_1, \cdots, \mathcal{Q}_p$,

and

(ii) $\mathcal{P}(-1)_1, \cdots, \mathcal{P}(-1)_p$ depend symmetrically on $\mathcal{P}_1, \cdots, \mathcal{P}_p$.

We wish to recall at this place the geometric description of the fundamental divisor relation $(\mathfrak{P}_p\mathfrak{R}_p^{-1})(\mathfrak{Q}_p\mathfrak{R}_p^{-1})(\mathfrak{S}_p\mathfrak{R}_p^{-1}) \approx 1$.

Let $\mathfrak{A}_{3p}$ be an arbitrary class of degree $3p$, its dimension $\dim \mathfrak{A}_{3p}$ is equal to $2p+1$ according to the theorem of Riemann-Roch. By means of the given class $\mathfrak{A}_{3p}$ the function field K can be represented by curve C_{3p} of the $2p$-dimensional projective space $P_{2p}(k)$ over the underlying field k. The curve C_{3p} is of order $3p$ since K is an extension of degree $3p$ over any rational field $k(z)$ whose transcendental element z is the quotient of two inequivalent relatively prime integral divisors of $\mathfrak{A}_{3p}$. The hyperplanes H_{2p} of $P_{2p}(k)$ cut out on C_{3p} the groups of $3p$ points which space up the complete linear series $\mathfrak{A}_{3p}$.

Let now $\mathcal{P}_1, \cdots, \mathcal{P}_p$ and $\mathcal{Q}_1, \cdots, \mathcal{Q}_p$ be two generic p-tuples of points on C_{3p}. Since the imbedding space has dimension $2p$ there exists exactly one hyperplane $H_{2p}(\mathcal{P}_1, \cdots, \mathcal{P}_p; \mathcal{Q}_1, \cdots, \mathcal{Q}_p)$ passing through the $2p$ points. The remaining intersections of $H_{2p}(\mathcal{P}_1, \cdots, \mathcal{P}_p; \mathcal{Q}_1, \cdots, \mathcal{Q}_p)$ with C_{3p} are then a p-tuple $\mathcal{S}_1, \cdots, \mathcal{S}_p$ such that $\mathfrak{P}_p\mathfrak{Q}_p\mathfrak{S}_p \approx \mathfrak{A}_{3p}$. Obviously, $\mathcal{S}_1, \cdots, \mathcal{S}_p$ depend upon the class $\mathfrak{A}_{3p}$ which we have chosen for the construction. Since any other class $\mathfrak{A}'_{3p}$ can be obtained from $\mathfrak{A}_{3p}$ by multiplication with a suitable class $\mathfrak{C}$ of degree 0 we see that the geometric construction is consistent with the results obtained by making use of the multiplicative relation

$$(\mathfrak{P}_p\mathfrak{R}_p^{-1})(\mathfrak{Q}_p\mathfrak{R}_p^{-1})(\mathfrak{S}_p\mathfrak{R}_p^{-1}) \approx 1.$$

Since $\mathfrak{S}_p$, $\mathfrak{P}(-1)_p$ depend symmetrically on $\mathfrak{P}_p$ and $\mathfrak{Q}_p$, respectively, we can apply our results to the field of abelian functions $A = \mathcal{P}_1 \cdots \mathcal{P}_p$.

Let $\mathfrak{R}_p$ an arbitrary but fixed class of degree p. We can suppose that $\dim \mathfrak{R}_p = 1$ and $\mathfrak{R}_p$ is determined by $\mathfrak{r}_1 \cdots \mathfrak{r}_p$ where the $\mathfrak{r}_i$ are mutually dis-

tinct prime divisors of K. Let $\mathfrak{C}$ be an arbitrary divisor class of degree 0, then $\mathfrak{C} = \mathfrak{A}_p\mathfrak{R}_p^{-1}$ with a uniquely determined class $\mathfrak{A}_p$ of K. Consider the relation

$$\begin{aligned}(\mathfrak{P}_p\mathfrak{R}_p^{-1})\mathfrak{C} &\approx (\mathfrak{P}_p\mathfrak{R}_p^{-1})(\mathfrak{A}_p\mathfrak{R}_p^{-1}) \\ &\approx \mathfrak{P}_p\mathfrak{R}_p^{-1})(\mathfrak{a}_1 \cdots \mathfrak{a}_p\mathfrak{R}_p^{-1}) \\ &\approx (\mathfrak{P}(\mathfrak{C})_1 \cdots \mathfrak{P}(\mathfrak{C})_p\mathfrak{R}_p^{-1})\end{aligned}$$

where $\mathfrak{a}_1 \cdots \mathfrak{a}_p$ is an arbitrary integral divisor of $\mathfrak{A}_p$. The preceding remarks imply that

$$\dim (\mathfrak{P}(\mathfrak{C})_1 \cdots \mathfrak{P}(\mathfrak{C})_p) = 1, \text{ and}$$
$$\mathfrak{P}(\mathfrak{C})_1 \neq \mathfrak{P}(\mathfrak{C})_j \text{ if } i \neq j.$$

Hence the field $\mathfrak{P}(\mathfrak{C})_1 \cdots \mathfrak{P}(\mathfrak{C})_1 = A \circ \mathfrak{C}$ is contained in A. Since all classes of degree 0 in $K\Delta(\bar{\mathfrak{P}}_1, \cdots, \bar{\mathfrak{P}}_p)$, where $\bar{\mathfrak{P}}_i \cong K * I(\mathfrak{P}_i)$, form a group it follows that

$$(A \circ \mathfrak{C}) \circ \mathfrak{C}^{-1} \leqq A \circ \mathfrak{C} \leqq A,$$

hence

$$A \circ \mathfrak{C} = \mathrm{A}.$$

In other words, the field of abelian functions A admits a group of birational transformations which is isomorphic with the class group $\mathbf{D}$ of K.

This group of birational transformations does not depend on the choice of the reference divisor $\mathfrak{a}_1 \cdots \mathfrak{a}_p$ for the uniquely determined class $\mathfrak{P}_p\mathfrak{C}$ is equal to the class generated by $\mathfrak{P}(\mathfrak{C})_1 \cdots \mathfrak{P}(\mathfrak{C})_p$. We shall call this group of birational transformations $\mathbf{T}$ the group of translations.

Let $\Sigma_p(C)$ a model of the field A and let τ be an arbitrary but fixed translation. Then τ has certain fundamental points and fundamental varieties on $\Sigma_p(C)$. The map $\boldsymbol{M}(\mathfrak{A}_p, C)\tau$ of a variety $\boldsymbol{M}(\mathfrak{A}_p, C)$ is defined as the set of all points on $\Sigma_p(C)$ which satisfy the defining relations of τ. Obviously $\boldsymbol{M}(\mathfrak{A}_p, C)\tau = \boldsymbol{M}(\mathfrak{A}_p\tau, C)$ consists of all integral divisors in $\mathfrak{A}_p\tau = \mathfrak{A}_p\mathfrak{C}$ where τ is given by the class C. Consequently, $\mathbf{T}$ is a group of translations on the set $\boldsymbol{W}(K)$. We derive from $\boldsymbol{W}(K)$ an additive group $\boldsymbol{W}(K; \mathfrak{R}_p)$ relative to a fixed reference divisor class $\mathfrak{R}_p$. The relations

$$(\mathfrak{X}_p\mathfrak{R}_p^{-1})(\mathfrak{Y}_p\mathfrak{R}_p^{-1}) \approx (\mathfrak{Z}_p\mathfrak{R}_p^{-1})$$

can be used to define an addition $\oplus$ on $\boldsymbol{W}(K)$ relative to $\mathfrak{R}_p$. We define

$$\mathfrak{X}_p \oplus \mathfrak{Y}_p = \mathfrak{Z}_p, \text{ and}$$
$$\mathfrak{R}_p \text{ as the zero element,}$$

The additive group arising in such a fashion from $\boldsymbol{W}(K)$ shall be denoted by $\boldsymbol{W}(K; \mathfrak{R}_p)$. The addition of the varieties $\boldsymbol{M}(\mathfrak{X}_p)$, $\boldsymbol{M}(\mathfrak{Y}_p)$ is given by

$$\boldsymbol{M}(\mathfrak{X}_p) \oplus \boldsymbol{M}(\mathfrak{Y}_p) = \boldsymbol{M}(\mathfrak{Z}_p)$$

when

$$\mathfrak{X}_p \oplus \mathfrak{Y}_p = \mathfrak{Z}_p.$$

Obviously, $\boldsymbol{W}(K;\mathfrak{R}_p)$ is isomorphic with $\boldsymbol{D}$. The group $\mathbf{T}$ can be considered as operator group on $\boldsymbol{W}(K;\mathfrak{R}_p)$. It will be transitive on $\boldsymbol{W}(K;\mathfrak{R}_p)$. Namely, any two elements $\boldsymbol{M}(\mathfrak{X}_p)$ and $\boldsymbol{M}(\mathfrak{Y}_p)$ determine as translation τ such that $\boldsymbol{M}(\mathfrak{X}_p)\tau = \boldsymbol{M}(\mathfrak{Y}_p)$. The class $\boldsymbol{C}$ which determines τ is given as $\mathfrak{Y}_p\mathfrak{X}_p^{-1}$.

Remark. Using the general formulae for the multiplication $(\mathfrak{P}_p\mathfrak{R}_p^{-1})\boldsymbol{C}$ or the general theory of correspondences, it follows that the points on $\boldsymbol{\Sigma}_p(C)$ which are fundamental for the translation τ form an algebraic variety of dimension $< p-1$ on $\boldsymbol{\Sigma}_p(C)$.

The relation $(\mathfrak{P}_p\mathfrak{R}_p^{-1})(\mathfrak{P}(-1)_p\mathfrak{R}_p^{-1}) \approx 1$ gives rise to a new birational transformation ρ of the field of abelian functions A. Since the equation relating $\mathfrak{P}_p$ and $\mathfrak{P}(-1)_p$ is symmetric it follows that ρ has period 2: $\mathfrak{P}(-1)(-1)_p = \mathfrak{P}_p$. The previous remarks concerning the class $\mathfrak{P}(-1)_p$ imply that the field $\boldsymbol{\Sigma}_p(\mathfrak{P}(-1)_p)$ = symmetric product of $K * I(\mathfrak{P}(-1)_1), \cdots,$ $K * I(\mathfrak{P}(-1)_p)$ coincides with A. Thus, ρ gives rise to a birational transformation of A. We call this transformation the reflection.

The reflection ρ gives rise to another transformation on the set $\boldsymbol{W}(K)$. We obviously have to define

$$\boldsymbol{M}(\mathfrak{A}_p)\rho = \boldsymbol{M}(\mathfrak{A}(-1)_p)$$

where

$$(\mathfrak{A}_p\mathfrak{R}_p^{-1})(\mathfrak{A}(-1)_p\mathfrak{R}_p^{-1}) \approx 1.$$

In order to prove that ρ is not contained in $\mathbf{T}$ we observe that would imply

$$\mathfrak{A}_p\rho = \mathfrak{A}(-1)_p = \mathfrak{A}_p\tau = \mathfrak{A}_p\mathfrak{C}$$

with a fixed class $\mathfrak{C}$ for all classes $\mathfrak{A}_p$. Hence $\mathfrak{C} = \mathfrak{A}_p^{-2}(\mathfrak{R}_p^{-2})^{-1}$ for all classes $\mathfrak{A}_p$. Or, all classes of degree 0 have period 2: $(\mathfrak{A}_p\mathfrak{B}_p^{-1})^2 \approx 1$ where $\mathfrak{B}_p$ denotes an arbitrary class of degree p. As a consequence of the theorem of Riemann-Roch it can be proved that there exist infinitely many classes $\mathfrak{B}_p$ of dimension 1. Consequently $\boldsymbol{D}$ is an infinite group. Thus our assumption would imply that there exist infinitely many classes of degree 0 which have period 2. But that is impossible as we shall prove later.

4. The abelian functions of the classical theory. Let S be an arbitrary algebraic Riemann surface and $K = k(x, y)$ the associated field of rational functions on S. Thus, we may suppose that S is spread out over the

complex x-plane. The places of S are in one to one correspondence with the prime divisors of the function field K. Let $\mathfrak{r}_1, \cdots, \mathfrak{r}_p$ be a fixed p-tuple of places on S and $\mathfrak{p}_1 \cdots \mathfrak{p}_p$ an arbitrary p-tuple of places varying in a complete linear series of degree p. Then the abelian sums $\sum_{i=1}^{p} \int_{\mathfrak{r}_i}^{\mathfrak{p}_i} d\boldsymbol{u}$ where $d\boldsymbol{u} = (du_1, \cdots, du_p)$ denotes a complex base for the differentials of first kind on S are the same modulo the $2p$ periods $\| \omega_{ij} \| = \Omega$ of S for different representatives $\mathfrak{p}_1, \cdots, \mathfrak{p}_p$ of the given complete linear series, according to Abel's theorem. Thus, any divisor class $\mathfrak{P}_p$ determines uniquely a vector $\boldsymbol{w} \bmod \Omega$:

$$\sum_{i=1}^{p} \int_{\mathfrak{r}_i}^{\mathfrak{p}_i} d\boldsymbol{u} \equiv \sum_{i=1}^{p} \int_{\mathfrak{r}_i}^{\mathfrak{p}'_i} d\boldsymbol{u} \equiv \boldsymbol{w} (\operatorname{mod} \Omega),$$

when $\mathfrak{p}_1 \cdots \mathfrak{p}_p$ and $\mathfrak{p}'_1 \cdots \mathfrak{p}'_p$ determine the same class $\mathfrak{A}_p$. Conversely, a general vector $\boldsymbol{w}$ determines a p-tuple of points $\mathfrak{p}_1, \cdots, \mathfrak{p}_p$ of S (Jacobi's inversion theorem). The explicit relationship between the vectors $\boldsymbol{w}$ and the groups $\mathfrak{p}_1, \cdots, \mathfrak{p}_p$ is given by the abelian functions of the classical theory. An abelian function of the classical theory is defined as a symmetric function of p places $\mathfrak{p}_1, \cdots, \mathfrak{p}_p$ which is a univalent meromorphic function of the p integrals of first kind $u_1, \cdots, u_p$. In order to prove that the field of classical $2p$-fold periodic abelian functions B coincides with the field of abelian functions A which we defined before, we refer to Weierstrass' solution of the inversion problem.[11] Weierstrass proves that B is generated by the symmetric function of the $2p$ functions

$$x_a = x * \mathfrak{P}_a = \Phi_a(u_1, \cdots, u_p)$$
$$y_a = y * \mathfrak{P}_a = \Psi_a(u_1, \cdots, u_p)$$

given by integrating the following system of differential equations

$$du_i = \sum_{a=1}^{p} H(x_a, y_a)_i \, dx_a \qquad (i = 1, \cdots, p)$$

where

$$f(x_a, y_a) = 0, \qquad (\alpha = 1, 2, \cdots, p),$$

and

$$\Phi_a(0, \cdots, 0) = x * \mathfrak{r}_a$$
$$\Psi_a(0, \cdots, 0) = y * \mathfrak{r}_a.$$

Thus for generic values of the argument $\boldsymbol{u} = (u_1, \cdots, u_p)$ the functions $\Phi_a = x_a$, $\Psi_a = y_a$ determine a generic point $\mathfrak{P}$ of the p-fold symmetric product

---

[11] K. Weierstrass, *Collected Papers*, vol. IV. H. F. Baker's ***Abel's Theorem and the Allied Theory, Including the Theory of Theta Functions*** (1897).

$\Sigma_p(S)$ of the Riemann surface S. Thus, $B = \mathfrak{P}_1 \cdots \mathfrak{P}_p$. Since $\Sigma_p(S)$ can be considered as representing the p-fold symmetric product of the projective model C, we have according to the definition of the generic point that

$$B = A.$$

The singular arguments $(u_1{}^0, \cdots, u_p{}^0)$ of the abelian functions of Φ_a, Ψ_a which form a variety whose complex dimension is at most equal to $p-1$, correspond to the classes A_p whose dimension is greater than 1. The field B consists of all rational functions in the parallelotop of periods $\bar{\Omega}$—the Jacobian variety—which when represented in a $2p$-dimensional real space is the closed group manifold of the group of translations T.

The manifolds $\boldsymbol{M}(\mathfrak{A}_p)$ of $\boldsymbol{W}(K)$ are thus in (1–1) correspondence with the vectors $\boldsymbol{W}$ mod Ω. The previously defined addition $\oplus$ on $\boldsymbol{W}(K)$ corresponds to addition of vectors mod Ω for Abel's theorem yields

$$\sum_{i=1}^{p}\int_{\mathfrak{r}_i}^{\mathfrak{p}_i} d\boldsymbol{u} + \sum_{i=1}^{p}\int_{\mathfrak{r}_i}^{\mathfrak{q}_i} d\boldsymbol{u} \equiv \boldsymbol{w}(\mathfrak{p}_1, \cdots, \mathfrak{p}_p) + \boldsymbol{w}(\mathfrak{q}_1, \cdots, \mathfrak{q}_p) \equiv \sum_{i=1}^{p}\int_{\mathfrak{r}_i}^{\mathfrak{s}_i} d\boldsymbol{u} \, (\mathrm{mod}\ \Omega).$$

Let $\mathfrak{P}_p$, $\mathfrak{Q}_p$, $\mathfrak{S}_p$, $\mathfrak{R}_p$ be the divisor classes which are associated to $\mathfrak{p}_1 \cdots \mathfrak{p}_p$, $\mathfrak{q}_1 \cdots \mathfrak{q}_p$, $\mathfrak{s}_1 \cdots \mathfrak{s}_p$, $\mathfrak{r}_1 \cdots \mathfrak{r}_p$, respectively. Then

$$(\mathfrak{P}_p\mathfrak{R}_p{}^{-1})(\mathfrak{Q}_p\mathfrak{R}_p{}^{-1}) \approx (\mathfrak{S}_p\mathfrak{R}_p{}^{-1}).$$

The relation between $\bar{\Omega}$ and $\Sigma_p(S)$ can be expressed as follows: there exists a birational transformation between $\bar{\Omega}$ and $\Sigma_p(S)$ whose fundamental points on $\bar{\Omega}$ are the points lying on the singular manifold of the field of abelian functions B.

5. The natural multiplications of the field of abelian functions. Let $\boldsymbol{D}$ be the group of all divisor classes of degree 0 which belongs to the field $K = k(x, y)$. We want to prove that the number $\omega(k; n)$ of classes in $\boldsymbol{D}$ whose order is a (proper or improper) divisor of n, is finite. First we reduce the problem to a question related to a fixed class of degree 0. Let $\mathfrak{C} = \mathfrak{X}_p\mathfrak{Q}_p{}^{-1}$ be an arbitrary class of degree 0 and $\mathfrak{r}_1 \cdots \mathfrak{r}_p$ an arbitrary non-special divisor of degree p. Let $\omega(k; n; \mathfrak{C})$ be the number of classes $\mathfrak{Y}_p\mathfrak{R}_p{}^{-1}$ for which $(\mathfrak{Y}_p\mathfrak{R}_p{}^{-1})^n(\mathfrak{X}_p\mathfrak{Q}_p{}^{-1}) \approx 1$. Obviously, $\omega(k; n; \mathfrak{C})$ is equal to the number of classes $\mathfrak{C}_i$ satisfying the equation $\mathfrak{C}_i{}^n \approx \mathfrak{C}^{-1}$. Suppose now that $\mathfrak{C}^* = \mathfrak{Y}_p{}^*\mathfrak{Q}^*{}_p{}^{-1}$ is another class of degree 0. Let $\omega(k; n; \mathfrak{C}^*)$ be the number of solutions of $(\mathfrak{Y}^*{}_p\mathfrak{R}_p{}^{-1})(\mathfrak{X}^*{}_p\mathfrak{Q}^*{}_p{}^{-1}) \approx 1$. If $\mathfrak{C}_1$, $\mathfrak{C}_2$ denote two different solutions of $\mathfrak{C}^n \approx \mathfrak{C}^{-1}$—provided they exist—then $(\mathfrak{C}_1\mathfrak{C}_2{}^{-1})^n \approx 1$. Hence

$$(\mathfrak{Y}^*_p\mathfrak{R}_p^{-1})^n(\mathfrak{X}^*_p\mathfrak{Q}^*_p{}^{-1}) \approx (\mathfrak{C}_1\mathfrak{C}_2^{-1})^n(\mathfrak{Y}^*_p\mathfrak{R}_p^{-1})^n(\mathfrak{X}^*_p\mathfrak{Q}^*_p{}^{-1})$$
$$\approx (\mathfrak{C}_1\mathfrak{C}_2^{-1}\mathfrak{Y}^*_p\mathfrak{R}_p^{-1})^n(\mathfrak{X}^*_p\mathfrak{Q}^*_p{}^{-1}) \approx 1, \text{ i.e.}$$
$$\omega(k;n;\mathfrak{C}) \leqq \omega(k;n;\mathfrak{C}^*).$$

In the same fashion it follows that $\omega(k;n;\mathfrak{C}^*) \leqq \omega(k;n;\mathfrak{C})$, consequently $\omega(k;n;\mathfrak{C}) = \omega(k;n;\mathfrak{C}^*) = \omega(k;n)$.

Thus, it suffices to show that $\omega(k;n;\mathfrak{C})$ is finite for a special class C. For this purpose we formulate the problem as a problem concerning the adjoint curves ψ of a model $C(x,y)$ of $K = k(x,y)$ which is given by an irreducible separable equation $f(x,y) = 0$. The curve $C(x,y)$ has only a finite number of singularities; it has order m if $[K:k(x)] = m$. An adjoint curve ψ of order v is a curve of the (x,y)-plane which passes through the singular points of $C(x,y)$ with the right multiplicities.[12]

Suppose now that we already found an adjoint curve ψ of order v which has the following properties:[13]

i) it passes through the multiple points of $f(x,y) = 0$,

ii) it passes through the points $\mathfrak{q}_1, \cdots, \mathfrak{q}_q$, $\mathfrak{b}_1, \cdots, \mathfrak{b}_s$ of $C(x,y)$ and

iii) has n-fold contacts with $C(x,y)$ in p points $\mathfrak{r}_1, \cdots, \mathfrak{r}_p$.

We want to determine another *adjoint* curve ϕ of the same order v which satisfies the following conditions:

iv) it passes through $\mathfrak{b}_1, \cdots, \mathfrak{b}_s$,

v) it passes through q other points $\mathfrak{x}_1, \cdots, \mathfrak{x}_q$ on $C(x,y)$ and

vi) it has n-fold contacts with $C(x,y)$ in p points $\mathfrak{y}_1, \cdots, \mathfrak{y}_p$.

Fix for this purpose an arbitrary point (α,β) in the (x,y)-plane and consider the pencil $L(\alpha,\beta;\lambda) = 0$ of lines with the center (α,β). Draw the lines issuing from the center and passing through the vm intersections. The parameter λ_j describing these vm lines satisfy an equation $F_{vm}(\lambda) = 0$ of degree vm which is obtained by eliminating x from

$$\phi = 0, \quad f = 0, \quad L(\alpha,\beta;\lambda) = 0.$$

---

[12] F. Severi, *Trattato di geometria algebraica* (1926).

[13] A. Clebsch and P. Gordan, *Theorie der Abelschen Funktionen*, p. 231 (1866).

The factors $(\lambda - \lambda_j)$ of $F_{\nu m}(\lambda) = 0$ which correspond to the points classified under (i) and (ii) are known. Hence

$$F_{\nu m}(\lambda)[\prod_{(i),(ii)} (\lambda - \lambda_j)]^{-1} = F_{np}(\lambda) = 0$$

determines the lines drawn to the remaining intersections (iii). The subscripts (i), (ii) in the product that we formed, indicate the product over all $\lambda - \lambda_j$ which correspond to the points enumerated in (i) and (ii). As long as n is relatively prime to the characteristic χ of k there is no difficulty in counting the multiplicities according to theory of resultants. Consequently, condition (iii) implies that $F_{np}(\lambda)$ has p roots each of which is counted with the multiplicity n. Hence

$$F_{np}(\lambda) = F_p(\lambda)^n.$$

Thus $F_p(\lambda) = 0$ furnishes the p points of contact.

Now let $\phi_0, \phi_1, \cdots, \phi_{(n-1)p}$ be the $(n-1)p+1$ linearly independent curves of order ν passing through the points mentioned under (ii) and (iii). The curve ϕ must then have the equation $\phi = \phi(\{c\}) = \sum_{i=0}^{(n-1)p} c_i\phi_i$, $c_i \epsilon k$. Therefore

$$F_{m\nu}(\lambda) = F_{m\nu}(\lambda; \{\epsilon\})$$

or precisely

$$F_{m\nu}(\lambda) = F_{m\nu}(\lambda; c_1c_0^{-1}, \cdots, c_{(n-1)p}c_0^{-1}),$$

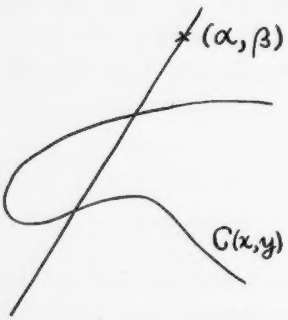
$F_{m\nu}(\lambda)$ involving the ratios $c_ic_0^{-1}$ $(i = b, \cdots, (n-1)p)$ in a rational fashion. Thus

$$F_{m\nu}(\lambda; \{c\}) = F^*(\lambda)F_{np}(\lambda; \{c\})$$

where the factor $F^*(\lambda)$ corresponds to the intersections (i), (ii), i.e. it does not depend on $\{c\}$.

We require $F_{np}(\lambda; \{c\}) = F_p(\lambda; \{c\})^n$. Thus we obtain relations for the $(n-1)p$ ratios $c_ic_0^{-1}$. Now change $\mathfrak{q}_1, \cdots, \mathfrak{q}_q$ to $\mathfrak{x}_1, \cdots, \mathfrak{x}_q$ and take care of the conditions (iv) and (vi). Under these circumstances $F_{np}(\lambda; \{c\})$ involves the ratios $c_ic_0^{-1}$ and the coördinates of the points $x_1, \cdots, x_q$ in a rational fashion. The required relation $F_{np}(\lambda; \{c\}) = F_p(\lambda; \{c\})^n$ implies $(n-1)p$ relations for the coefficients $c_ic_0^{-1}$. For $F_p(\lambda; \{c\})$ contains $p+1$ coefficients, comparing coefficients on both sides of the postulated equation yields $np+1$ equations to hold between the $p+1$ coefficients of $F_p(\lambda; \{c\})$ and the quantities $c_ic_0^{-1}$. Eliminating the $p+1$ coefficients, we obtain $(n-1)p$ relations

for the ratios $c_i c_0^{-1}$. Next we eliminate from these equations the ratios $c_2 c_0^{-1}, \cdots, c_{(n-1)p} c_0^{-1}$ and thus obtain an equation for $c_1 c_0^{-1} = t$. The roots t_j of this equation determine in general the curves ϕ satisfying the desired properties iv), v) and vi). However, for certain positions of the center (α, β) it may happen that the line belonging to a particular solution t_j does not determine a point of n-fold contact. Namely, the line may intersect $C(x, y)$ in more than one point. E. G. the particular line is counted twice but does not furnish a 2-fold contact since the points of intersection are different. Such centers are exceptional, in order to obtain adjoint curves ϕ which satisfy the required conditions we form the greatest common divisor $(G_{\alpha_\mu, \beta_\mu}(t), \cdots) = H(t)$ for all positions (α_μ, β_μ) of the center. The roots of $H(t) = 0$ determine then exactly the adjoint curves which have n-fold contacts and are restrained by the conditions iv), v) and vi). We can obtain $H(t) = 0$ also by considering a generic point $(\bar{\alpha}, \bar{\beta})$ of the (x, y)-plane and consider the roots of $G_{\bar{\alpha}, \bar{\beta}}(t) = 0$ which do not depend on the parameters of $(\bar{\alpha}, \bar{\beta})$; i. e. we consider the algebraically closed field of the field of parameters $k(\alpha)$ as underlying ground field. Thus $\omega(k; n)$ is the degree of $H(t) = 0$.



A simple consequence of the preceding considerations is the following. Let L^* be an arbitrary algebraically closed transcendental extension of k which is algebraically independent of K. Consider the field KL^* and its group $\boldsymbol{D}^*$ of divisor classes of degree 0. By the same considerations as before it can be shown that $\omega(L^*, n)$ is finite. Assuming that n is relatively prime to the characteristic χ of the underlying field of coefficients k it follows at once by going over the previous proof of the finiteness of $\omega(k; n)$ that $\omega(L^*, n) = \omega(k; n)$. In particular, let $f(x, y) = 0$ be a defining equation of the field K relative to k and let k_0 be the algebraically closed extension of the prime field which is contained in k. Then $f(x, y) = \Sigma a_{ij} x^i y^j$ may involve a certain number of quantities a_{ij} which are transcendental over k_0. Adjoining to k_0 these elements and form the algebraic closure $k_1 = \overline{k(a_{ij})}$ in k. Then $f(x, y) = 0$ defines a function field $K_1 = k_1(x, y)$ over k_1 which has the same genus p as K; $K_1 k = K$. Applying the formula $\omega(n; L^*) = \omega(k; n)$ to this special case we see that $\omega(k_1; n) = \omega(k; n)$; i. e. the number of classes of degree 0 which have the same order n—$(n, \chi) = 1$—depends only on the smallest algebraically closed field determined by the defining equation $f(x, y) = 0$ of K. Of course, the fields k_1 depend on the selection of the defining equation $f(x, y) = 0$.

If n is equal to a power χ^μ of the characteristic χ then is also finite, as has been shown by H. Hasse and E. Witt.[14]

Remark. In particular, $\omega(k;2)$ is finite. Thus, as we pointed out before, the reflection ρ is not contained in the group of translations $\mathbf{T}$.

Let $\boldsymbol{D}_n$ be the finite abelian group of order $\omega(k;n)$ which consists of all divisor classes of degree whose order is equal to n. The elements of $\boldsymbol{D}_n$ include translations τ_n of finite order n on the abelian function field $\boldsymbol{A}$. Thus, A admits for each integer n a finite group of automorphisms $\mathbf{T}_n$ given by

$$(\mathfrak{P}_1\cdots\mathfrak{P}_p\mathfrak{R}_p^{-1})\mathfrak{C}_n \approx \mathfrak{P}_1\tau_n\cdots\mathfrak{P}_p\tau_n\mathfrak{R}_p^{-1},$$

where $\mathfrak{C}_n$ denotes the divisor class of order n which induces the particular transformation τ_n. All functions of A which are left invariant by the translations of $\mathbf{T}_n$ constitute according to the Galois theory a subfield A_n of A. The Galois group of A with respect to A_n is abelian and isomorphic with $\mathbf{T}_n$.

The field A is an unramified extension of A_n provided that we measure ramifications with respect to the set $\boldsymbol{W}(K)$. Using a fixed reference class $\mathfrak{R}_p$ we showed before that $\boldsymbol{W}(K)$ considered as an additive group is isomorphic with $\boldsymbol{D}$. Since each class $\mathfrak{C}$ of $\boldsymbol{D}$ has exactly $\omega(k;n)$ conjugate elements $\mathfrak{C}\tau_n = \mathfrak{C}\mathfrak{C}_n$ it follows that each element of $\boldsymbol{W}(K)$ has $\omega(k;n) = [A:A_n]$ conjugates; i. e. A is an unramified extension of A_n. Each group $\boldsymbol{D}_n$ determines an algebraic involution of order $\omega(k;n)$ on A. If $n=\chi^\mu$ then $\boldsymbol{D}_n$ can be equal to unity.

Next, consider the generic class $\mathfrak{P}_1\cdots\mathfrak{P}_p\mathfrak{R}_p^{-1}$ of $\boldsymbol{D}$ interpreted as a class of degree 0 belonging to the extended function field $\bar{K}L$. Raise $\mathfrak{P}_1\cdots\mathfrak{P}_p\mathfrak{R}_p^{-1}$ to the n-th power, then

$$(\mathfrak{P}_1\cdots\mathfrak{P}_p\mathfrak{R}_p^{-1})^n \approx \mathfrak{P}(n)_1\cdots\mathfrak{P}(n)_p\mathfrak{R}_p^{-1}.$$

The resulting transformation $A=\mathfrak{P}_1\cdots\mathfrak{P}_p \rightarrow \mathfrak{P}(n)_1\cdots\mathfrak{P}(n)_p = A^{(n)}$ is a rational transformation of the field of abelian functions upon a subfield $A^{(n)}$. The rationality of the transformation follows from the fact that for suitable specializations $\mathfrak{P}_i \rightarrow \mathfrak{p}_i$ the corresponding prime divisors $\mathfrak{p}(n)_1,\cdots,\mathfrak{p}(n)_p$ are uniquely determined. Hence $[x * \mathfrak{P}(n)_i]$ are rational functions of $\Delta_p(K) \subset L$. Moreover $[x * \mathfrak{P}(n)_i]$, $i=1,\cdots,p$, generate p algebraically independent function fields which are isomorphic to K. Thus $A^{(n)}$ has the degree of transcendency p with respect to k. Obviously $A^{(n)} \cong A$ according

[14] H. Hasse and E. Witt, "Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p," *Monatshefte für Mathematik und Physik*, vol. 43 (1936).

to construction. This isomorphism implies that A is a finite algebraic extension of $A^{(n)}$. The field $A^{(n)}$ is called the field obtained from A by natural multiplication with n.

Since $\boldsymbol{D}_n$ is contained in the class group $\boldsymbol{D}^*$ which belongs to $\bar{K}L$, it follows $\boldsymbol{D}_n \subseteqq \boldsymbol{D}^*_n$. Consequently $(\mathfrak{P}(n)_1 \cdots \mathfrak{P}(n)_p)\tau_n = (\mathfrak{P}(n)_1 \cdots \mathfrak{P}(n)_p$ for

$$(\mathfrak{P}_1 \cdots \mathfrak{P}_p \mathfrak{R}_p^{-1})^n \mathfrak{C}^*{}_n{}^n \approx (\mathfrak{C}^*{}_n \mathfrak{P}_1 \cdots \mathfrak{P}_p \mathfrak{R}_p^{-1})^n \approx (\mathfrak{P}_1 \cdots \mathfrak{P}_p \mathfrak{R}_p^{-1})^n$$
$$\approx \mathfrak{P}(n)_1 \cdots \mathfrak{P}(n)_p \mathfrak{R}_p^{-1}.$$

Thus

$$A_n \geqq A^{(n)}.$$

If $n = \chi^\mu$ then one can exhibit examples of fields K such that $A_n > A^{(n)}$ and even $A = A_n$.

We formulate our result again:

The field $A^{(n)} \leqq A_n$ obtained from A by multiplication with n is isomorphic with A. The field A is an abelian unramified extension of A_n whose Galois group is isomorphic with the group of translations T_n of finite order n.

6. The natural multiplications in the classical theory of abelian functions. Suppose now that the underlying field of constants k is the field of all complex numbers. The associated field A of abelian functions shall be given by $p+1$ linearly independent $2p$-fold periodic functions $\mathrm{A}_1(u_1, \cdots, u_p; \Omega), \cdots, \mathrm{A}_{p+1}(u_1, \cdots, u_p; \Omega)$ of the p integrals of first kind on K. The classes of $\boldsymbol{D}_n$ form in this case an abelian group of order n^{2p} possessing $2p$ generators $\tau(n)_{jl}$ of exact order n. These generators $\tau(n)_{jl}$ correspond to the divisor classes representing the solutions of $\sum_{i=1}^{p} \int_{r_i}^{p_i} d\boldsymbol{u} \equiv n^{-1}\omega_{jl} (\mathrm{mod}\ l)$ where $\Omega = \| \omega_{jl} \|$, $j = 1, 2$; $l = 1, \cdots, p$ represent a generating system of periods of the integrals of first kind. The field A_n consists then of all abelian functions which are left invariant by the automorphisms induced by $\tau(n)_{jl}$. We define $\tau(n)_{jl}$ on A by the mappings

$$\{\mathrm{A}_1(u_1, \cdots, u_p; \Omega), \cdots, \mathrm{A}_{p+1}(u_1, \cdots, u_p; \Omega)\}$$
$$\rightarrow \{\mathrm{A}_1(u_1, \cdots, u_p; \Omega), \cdots, \mathrm{A}_{p+1}(u_1, \cdots, u_p; \Omega)\}\tau(n)_{jl}$$

$$= \{\mathrm{A}_1(u_1, \cdots, u_l + n^{-1}\omega_{jl}, \cdots, u_p; \Omega), \cdots, A_{p+1}(u_1, \cdots, u_l + n^{-1}\omega_{jl}, \cdots, u_p; \Omega)\}.$$

Hence according to the Galois theory A is an abelian extension of degree n^{2p} over A_n, the Galois group is isomorphic with the direct product of $2p$ cyclic groups of order n. According to the construction the functions A_n are $2p$-fold periodic functions whose periods are given by $\Omega n^{-1} = \| \omega_{jl} n^{-1} \|$. The field

A_n coincides therefore with the field $A^{(n)}$ consisting of all rational functions of $\{\mathrm{A}_1(nu_1, \cdots, nu_p; \Omega), \cdots, \mathrm{A}_{p+1}(nu_1, \cdots, nu_p; \Omega)\}$ i. e. the abelian functions obtained by multiplying the arguments by the integer n. Namely $\mathrm{A}_i(u_1, \cdots, u_l + n^{-1}\omega_{jl}, \cdots, u_p; \Omega)$ has the property

$$\begin{aligned}&\mathrm{A}_i(nu_1, \cdots, n(ul + n^{-1}\omega_{jl}), \cdots, nu_p; \Omega)\\ &\quad = \mathrm{A}_i(nu_1, \cdots, nu_l, \cdots, nu_p; \Omega), \qquad (i = 1, \cdots, p+1).\end{aligned}$$

Obviously, $A^{(n)} \cong A_n$.

Suppose now that $K_1 = k_1(x, y)$ is a field of algebraic functions of genus p over an arbitrary algebraically closed field k of characteristic 0. We want to prove that the number $\omega(k; n)$ is equal to n^{2p}. Let $\bar{a}$ be the field of all algebraic numbers, then k_1 contains a subfield a which is isomorphic with $\bar{a}$. Assume that K_1 is defined by an irreducible equation $f(x, y) = \Sigma t_{ij} x^i y^j = 0$, $t_{ij} \in k_1$. Denote by k_2 the least algebraically closed field containing $a(\{t_{ij}\})$, $k_2 \subseteqq k_1$. Since k_2 is a field of algebraic functions of a finite number of variables $t_1, \cdots, t_\lambda$ $(\lambda \geqq 0)$ over the field a we may suppose that the transcendental base $t_1, \cdots, t_\lambda$ consists of certain elements t_{ij} appearing in $f(x, y) = 0$. Next choose a set of complex numbers $\bar{t}_1, \cdots, \bar{t}_\lambda$ which are algebraically independent over $\bar{a}$. The algebraically closed field $\bar{k}_2$ of $\bar{a}(\bar{t}_1, \cdots, \bar{t}_\lambda)$ in the field of all complex numbers $\bar{k}$ is isomorphic with k_2. The equation $f(x, y) = \Sigma t_{ij} x^i y^j$ becomes $f(\bar{x}, \bar{y}) = \Sigma \bar{t}_{ij} \bar{x}^i \bar{y}^j$ where $\bar{t}_{ij}$ are the elements of $\bar{k}_1$ which correspond to the elements t_{ij} by means of the fixed isomorphism between $\bar{k}_2$ and k_2. The field $\bar{K} = \bar{k}_2(\bar{x}, \bar{y})$ is then isomorphic with $K_2 = k_2(x, y)$. Consequently, $\omega(k_2; n) = \omega(\bar{k}_2; n)$ and the respective groups of classes of order n are isomorphic. The defining equation $f(\bar{x}, \bar{y}) = 0$ remains irreducible in the field $\bar{k}$ of all complex numbers. Hence $\bar{K} = \bar{k}(\bar{x}, \bar{y}) = \bar{K}_2 \bar{k}$. We noticed before that $\omega(\bar{k}; n) = \omega(\bar{k}_2; n)$. Hence $\omega(\bar{k}_2; n) = n^{2p}$. We translate this result back to k_2 and obtain $\omega(k_2; n) = n^{2p}$. Now we apply the argument concerning the transcendental extensions of the ground field to the field $k_2(x, y) = K_2$. Thus $K_1 = k_1(x, y) = K_2 k_1$; K_1 and K_2 have the same defining equation hence their genera coincide. Moreover, $\omega(k_1; n) = \omega(k_2; n) = n^{2p}$. Thus we find that the group $\boldsymbol{D}_n$ of all classes of order n belonging to a function field $K_1 = k_1(x, y)$ of genus p over an arbitrary algebraically closed field k_1 of characteristic 0 is isomorphic with the direct product of $2p$ cyclic groups of order n.

The number $\omega(k; n)$ can be interpreted as an intersection number. Suppose that the field K is given by a model C without singularities in the projective 3-space over k. From the np-fold symmetric product of the curve C, it is a np-dimensional variety V_{np} which is represented in the direct np-fold product of the projective 3-space. The variety V_{np} obviously represents the

np-tuples of points on C, i. e. the np-tuples $\mathfrak{q}_1, \cdots, \mathfrak{q}_{np}$ of prime divisors $\mathfrak{q}_i$ of K. Let $\mathfrak{r}_1 \cdots \mathfrak{r}_p = \mathfrak{R}_p$ be an arbitrary divisor of degree p. Then $\mathfrak{R}_p{}^n$ has the dimension $(n-1)p+1$. The integral divisors of $\mathfrak{R}_p{}^n$ form a variety $V_{(n-1)p}$ of dimension $(n-1)p$ which lies on V_{np}. Consider next the variety V_p of dimension p which spanned up by all divisors $(\mathfrak{p}_1 \cdots \mathfrak{p}_p)^n$ where the $\mathfrak{p}_i$ are arbitrary prime divisors of K. Then the divisors $(\mathfrak{p}_1 \cdots \mathfrak{p}_p \mathfrak{R}_p{}^{-1})^n$ which are divisors of functions in K correspond to the points of the intersection $V_p \cap V_{(n-1)p}$. Namely, if $\mathfrak{P} \in V_p \cap V_{(n-1)p}$ then

i) $\mathfrak{P} \in V_p$ i. e. $\mathfrak{P}$ is given as $(\mathfrak{p}_1 \cdots \mathfrak{p}_p)^n$ and

ii) $\mathfrak{P} \in V_{(n-1)p}$ i. e. $\mathfrak{P}$ is given by an integral divisor of $\mathfrak{R}_p{}^n$.

Hence $(\mathfrak{p}_1 \cdots \mathfrak{p}_p \mathfrak{R}_p{}^{-1})^n \approx 1$. If the class $\mathfrak{r}_1 \cdots \mathfrak{r}_p$ is sufficiently general it follows that the intersection $V_p \cap V_{(n-1)p}$ has dimension 0. Consequently, the different points of intersection correspond to the classes $\mathfrak{P}_p$ which are determined by $\mathfrak{p}_1 \cdots \mathfrak{p}_p$ for which $\mathfrak{P}_p{}^n \approx \mathfrak{R}_p{}^n$. Moreover, $\omega(k; n) = \deg V'_p \times \deg V'_{(n-1)p}$ provided that V_p and $V_{(n-1)p}$ are represented by suitably chosen birationally equivalent varieties V'_p and $V'_{(n-1)p}$ respectively, in a linear space. We remark that this interpretation of the problem yields a normalization of the unramified multiplicative functions of order n on the associated Riemann surface S.

THE JOHNS HOPKINS UNIVERSITY.

SIMULTANEOUS REDUCTION OF A SQUARE MATRIX AND AN HERMITIAN MATRIX TO CANONICAL FORM.*

By JOHN WILLIAMSON.

It is well known that, if A is a square matrix with elements in the complex number field, there exists a unitary matrix U satisfying

$$UAU^* = T, \tag{1}$$

where T is a triangular matrix, i. e. a matrix all of whose elements lying to the left of the leading diagonal are zero.[1] Similarly, if the elements of A are real numbers, there exists a real orthogonal matrix O, such that

$$OAO' = T_1.\text{[2]} \tag{2}$$

The matrix T_1, while not a triangular matrix, is a matrix of the following form. It may be written as a matrix of matrices,

$$T_1 = (t_{ij}), \qquad (i, j = 1, 2, \cdots, m), \tag{3}$$

where t_{ij} is a matrix of e_i rows and e_j columns. If k is the number of real characteristic roots of A and r the number of pairs of complex conjugate roots, exactly k of the e_i have the value one and exactly r the value two. Further $t_{ij} = 0$, when $i > j$.

The above two results may be stated in a slightly different form. If H is a definite non-singular hermitian matrix, there exists a non-singular matrix P such that

$$PHP^* = \epsilon E, \tag{4}$$

where E is the unit matrix and $\epsilon = \pm 1$. Then, if B is any square matrix and

$$PBP^{-1} = A,$$

it follows from (1) that

$$UPBP^{-1}U^* = T,$$

or since U is unitary that,

$$UPB(UP)^{-1} = T.$$

* Received May 17, 1938.

[1] Aurel Wintner, *Spektraltheorie der unendlichen Matrizen* (1929), p. 29.

[2] F. D. Murnaghan and Aurel Wintner, *Proceedings of the National Academy of Science*, vol. 17 (1931), pp. 417-420.

In addition, as a consequence of (4),

$$UPH(UP)^* = \epsilon E.$$

Hence we have the result I: *If B is a square matrix with elements in the complex number field and H is a non-singular definite hermitian matrix, there exists a non-singular matrix C, such that*

$$CBC^{-1} = T \quad \text{and} \quad CHC^* = \epsilon E,$$

where T is a triangular matrix and $\epsilon = \pm 1$.

Similarly, if B is a matrix over the field of all real numbers and H is a non-singular definite real symmetric matrix, there exists a real non-singular matrix C, such that

$$CBC^{-1} = T_1 \quad \text{and} \quad CHC' = \epsilon E,$$

where T_1 is the matrix of equation (3).

The simplicity of these two results depends essentially, as we shall see, on the definite-ness of the matrix H. It is our purpose here to consider the corresponding problem when H is not definite, and in fact when H is a general hermitian or anti-hermitian matrix with elements that lie in an arbitrary field.

1. Let K be a field, of characteristic χ, over which is defined an automorphism of period one or two. If under this automorphism an element a of K corresponds to an element $\bar{a}$ of K, $\bar{\bar{a}} = a$. If $A = (a_{ij})$ is a matrix with elements in K, by A^* we shall mean the matrix (a^*_{ij}), where $a^*_{ij} = \bar{a}_{ji}$. In particular, if the automorphism over K is of period one, $A^* = A'$ the transposed of A. A matrix H is said to be hermitian, if $H^* = H$, and anti-hermitian if $H^* = -H$. Accordingly, when the automorphism over K is of period one, an hermitian matrix is symmetric, while an anti-hermitian is anti-symmetric (or skew-symmetric).[3]

Let

$$(5) \qquad C = (C_{ij}), \qquad (i, j = 1, 2, \cdots, r),$$

be a matrix of matrices, where C_{ij} is a matrix over K with e_i rows and e_j columns. If

$$D = (D_{ij}), \qquad (i, j = 1, 2, \cdots, r),$$

is a second such matrix, where D_{ij} is also a matrix of e_i rows and e_j columns,

[3] If $\chi = 2$ there is no distinction between an hermitian and an anti-hermitian matrix. For a more refined definition see A. A. Albert, "Symmetric and alternate matrices in an arbitrary field," *Transactions of the American Mathematical Society*, vol. 43 (May, 1938), no. 3, pp. 386-436.

we shall say that C and D are *similarly partitioned.* The matrix C in (5) is a *quasi-triangular* matrix if

(i) $C_{ij} = 0$, when $i > j$, and

(ii) the characteristic equation of C_{ii} is an irreducible polynomial of $K[x]$, $i = 1, 2, \cdots, r$.

When D is a second quasi-triangular matrix and D_{ii} is of the same order as C_{ii} for all values of i, we shall say that C and D are of the same type.

We first prove

LEMMA I. *If T is a non-singular triangular matrix and C a quasi-triangular matrix of the same order as T, then the matrix D, where $D = TCT^{-1}$, is a quasi-triangular matrix of the same type as C.*

Let

$$C = (C_{ij}),\quad T = (T_{ij}),\quad T^{-1} = (Q_{ij}),\quad D = (D_{ij}),\quad (i, j = 1, 2, \cdots, r),$$

be similar partitions of the four matrices, C, T, T^{-1} and D. Since T is a triangular matrix, if $i > j$, $T_{ij} = Q_{ij} = 0$, and since $D = TCT^{-1}$, $D_{ij} = 0$. Further, since $D_{ii} = T_{ii}C_{ii}Q_{ii}$ and $Q_{ii} = T_{ii}^{-1}$,

$$D_{ii} = T_{ii}C_{ii}T_{ii}^{-1}.$$

Hence D_{ii} is similar to C_{ii} and the characteristic equation of D_{ii} is the same as that of C_{ii} and so is irreducible. Therefore D is a quasi-triangular matrix of the same type as C.

Let A be a matrix over K and let the elementary factors of $A - xE$ be $(p_i(x))^{e_{ij}}$, where $p_i(x)$ is an irreducible polynomial of $K[x]$. If p_i is the companion matrix of $p_i(x)$, there exists a non-singular matrix B such that

$$BAB^{-1} = C = (C_{rs}), \qquad (r, s = 1, 2, \cdots, t), \tag{6}$$

where C is a quasi-triangular matrix and each C_{rr} is a matrix p_i.[4] The matrix C in (6) is of course a quasi-triangular matrix of a special form, since C_{rs} is zero when $s - r \geq 2$, but this fact is of no importance at present.

We are now in a position to give a more exact statement of the problem, in which we are interested. Let A be any square matrix over K and H a matrix over K, of the same order as A, which satisfies the equation

[4] J. H. M. Wedderburn, "Lectures on matrices," *Colloquium Publications* (1934), p. 29 and "The canonical form of a matrix," *Annals of Mathematics*, vol. 39 (1938), pp. 178-180.

$$(7) \qquad H^* = \epsilon H, \qquad \epsilon = \pm 1.$$

Let P be a non-singular matrix over K and let

$$(8) \qquad PAP^{-1} = A_1 \quad \text{and} \quad PHP^* = H_1.$$

We shall determine canonical forms for the matrices A_1 and H_1 in (8) analogous to the matrices T and ϵE of result *I*. In particular we shall show that A_1 is a quasi-triangular matrix and that H_1 is of a comparatively simple nature.

2. We proceed by considering a matrix

$$(9) \qquad S = (s_{ij}), \qquad (i, j = 1, 2, \cdots, m),$$

which satisfies

$$(10) \qquad S^* = \epsilon S, \qquad \epsilon = \pm 1.$$

Two distinct cases arise, (i) $s_{mm} \neq 0$ and (ii) $s_{mm} = 0$. In (i), since $s_{mm} \neq 0$, the matrix

$$(11) \qquad W = E - X,$$

where E is the unit matrix of order m and X is the matrix all of whose columns are zero except the last, which has the value $\{s_{1m}s_{mm}^{-1}, s_{2m}s_{mm}^{-1}, \cdots, s_{m-1,m}s_{mm}^{-1}, 0\}$ exists and is non-singular. A simple calculation shows that

$$(12) \qquad WSW^* = F = (f_{ij}), \qquad (i, j = 1, 2, \cdots, m),$$

where $f_{im} = f_{mi} = 0$, $i \neq m$ and $f_{mm} = s_{mm}$.

In case (ii), if $s_{mi} = 0$, $i = 1, 2, \cdots, m$, S is of the form F in (12) with $f_{mm} = 0$. We now suppose that $s_{mm} = s_{m-1,m} = \cdots s_{r+1,m} = 0$, $s_{rm} \neq 0$. Since, by (10), $\bar{s}_{mr} = \epsilon s_{rm}$, $s_{mr} \neq 0$. We replace the matrix X in (11) by

$$(13) \qquad X = (x_{ij}), \qquad (i, j = 1, 2, \cdots, m),$$

where

$$\begin{aligned}
x_{ij} &= 0, \; j \neq r, \; j \neq m, && (i = 1, 2, \cdots, m);\\
x_{ir} &= s_{im}s_{rm}^{-1}, && (i = 1, 2, \cdots, r-1);\\
x_{ir} &= 0, && (i = r, r+1, \cdots, m);\\
x_{im} &= (s_{ir}s_{rm} - s_{im}s_{rr})s_{rm}^{-1}s_{mr}^{-1}, && (i = 1, 2, \cdots, r-1);\\
x_{im} &= s_{ir}s_{mr}^{-1}, && (i = r+1, \cdots, m-1);\\
x_{rm} &= \tfrac{1}{2}s_{rr}s_{mr}^{-1}, \; \chi \neq 2; \; x_{rm} = 0, \; \chi = 2.
\end{aligned}$$

In place of (12) we now have

$$WSW^* = G = (g_{ij}), \qquad (i, j = 1, 2, \cdots, m), \tag{14}$$

where, when $\chi \neq 2$,

$$g_{rm} = s_{rm} \neq 0; \; g_{mr} = s_{mr} \neq 0; \; g_{rj} = g_{jr} = 0, \, j \neq m; \; g_{im} = g_{mi} = 0, \, i \neq r.$$

If $\chi = 2$, g_{rr} need not be zero. To prove (14), when $\chi \neq 2$, we re-arrange the rows and columns of the matrices S and W in the order $1, 2, \cdots, r-1, r+1, \cdots, r, m$ to obtain matrices Q and V respectively. The matrix Q has the form

$$Q = \begin{pmatrix} Q_{11} & Q_{12} \\ Q_{21} & Q_{22} \end{pmatrix} \quad \text{where} \quad Q_{22} = \begin{pmatrix} s_{rr} & s_{rm} \\ s_{mr} & 0 \end{pmatrix},$$

and V the form

$$V = \begin{pmatrix} E_{m-2} & -Q_{12}Q_{22}^{-1} \\ 0 & V_{22} \end{pmatrix} \quad \text{where} \quad V_{22} = \begin{pmatrix} 1 & -\frac{1}{2}s_{rr}s_{mr}^{-1} \\ 0 & 1 \end{pmatrix}.$$

Since $S^* = \epsilon S$, $Q^* = \epsilon Q$ and therefore

$$V^* = \begin{pmatrix} E_{m-2} & 0 \\ -Q_{22}^{-1}Q_{21} & V^*_{22} \end{pmatrix} \quad \text{where} \quad V^*_{22} = \begin{pmatrix} 1 & 0 \\ -\frac{1}{2}s_{rm}^{-1}s_{rr} & 1 \end{pmatrix}.$$

so that finally

$$VQV^* = \begin{pmatrix} Q_{11} - Q_{12}Q_{22}^{-1}Q_{21} & 0 \\ 0 & R_{22} \end{pmatrix} \quad \text{where} \quad R_{22} = \begin{pmatrix} 0 & s_{rm} \\ s_{mr} & 0 \end{pmatrix}. \tag{15}$$

By arranging the rows and the columns of the matrices in (15) in their original order we have (14). If $\chi = 2$, the same proof applies when the element $-\frac{1}{2}s_{rr}s_{mr}^{-1}$ of V_{22} is replaced by zero.

Let

$$R = (r_{ij}), \qquad (i, j = 1, 2, \cdots, n), \tag{16}$$

be a matrix which satisfies

$$R^* = \epsilon R.$$

and be of the following form. If $\chi \neq 2$ and k is any integer $m < k \leqq n$, there is at most one element different from zero in the k-th row and at most one element different from zero in the k-th column. Further if $r_{ik} \neq 0$ and $i < k$ every other element in the i-th row of R is zero and every element in the i-th column is zero except r_{ki}. If $\chi = 2$, R is of the same form except that when $r_{ik} \neq 0$ and $i < k$, r_{ii} need not be zero. We may write

$$R = \begin{pmatrix} R_{11} & R_{12} \\ R_{21} & R_{22} \end{pmatrix}, \tag{17}$$

where $R_{11} = S$ and S is given by (9). If $s_{mm} \neq 0$ and $\chi = 2$, it may happen that $r_{mk} \neq 0$ for some integer $k > m$. In this case R is a matrix of the form (16) in which m is replaced by $m - 1$. Otherwise, if $s_{mm} \neq 0$ the last row of R_{12} is zero. If

$$Y = \begin{pmatrix} W & 0 \\ 0 & E_{n-m} \end{pmatrix},$$

where W is given by (11),

$$YRY^* = \begin{pmatrix} WSW^* & WR_{12} \\ R_{21}W^* & R_{22} \end{pmatrix}.$$

Since the last row of R_{12} is zero, $XR_{12} = 0$ and $WR_{12} = R_{12}$. Since $R_{21}W^* = (WR_{12})^* = R^*{}_{12}$, $R_{21}W^* = R_{21}$. Therefore

$$YRY^* = \begin{pmatrix} F & R_{12} \\ R_{21} & R_{22} \end{pmatrix} = N, \tag{18}$$

where F is given by (12). It may happen that, as a consequence of the nature of R, the j-th row of S is zero. If this is so, the j-th row of X is also zero, so that the j-th row of WS and therefore the j-th row of $F = WSW^*$ are both zero. Since $F^* = \epsilon F$, the j-th column of F is zero. Hence the matrix N in (18) is of the same form as R in (16) except that m is replaced by $m - 1$.

If $s_{mm} = s_{m-1,m} = \cdots = s_{r+1,m} = 0$, $s_{rm} \neq 0$, we replace the matrix X in W by the matrix X of (13) and have

$$YRY^* = \begin{pmatrix} G & R_{12} \\ R_{21} & R_{22} \end{pmatrix} = N, \tag{19}$$

where G is given by (14). As in the previous case, if the j-th row of S is zero so is the j-th row of G. Moreover, if $\chi = 2$, and the j-th row of S is zero except for the element s_{jj}, the j-th row of G is zero except for the element $g_{jj} = s_{jj}$. Hence the matrix N in (19) is of the same form as the matrix R in (16) except that m is replaced by $m - 2$. If $s_{im} = 0$, $i = 1, 2, \cdots, m$, R is already of the form (16) with m replaced by $m - 1$. Since W is a non-singular triangular matrix, so is Y. Since the product of two triangle matrices is a triangular matrix, by the process of induction we have

LEMMA 2. *If $R = \epsilon R^*$, there exists a non-singular triangular matrix L such that*

$$LRL^* = M = (m_{ij}), \qquad (i, j = 1, 2, \cdots, n), \tag{20}$$

where, if $\chi \neq 2$, in any one row of M there is at most one element m_{rs} different from zero. If $\chi = 2$ and $m_{rs} \neq 0$, $r < s$, m_{rr} need not be zero.

Let $m_{rs} \neq 0$ and $r < s$. If D is the matrix obtained from the unit matrix by multiplying the r-th row by m_{rs}^{-1}, since $(m_{rs}^{-1})^* = \epsilon m_{sr}^{-1}$, the matrix DMD^* is obtained from M by replacing m_{rs} by 1, m_{sr} by ϵ and m_{rr} by $\epsilon m_{rr}/m_{sr}^{-1}m_{rs}^{-1}$. Hence we have the two lemmas

LEMMA 3. *The matrix M in (20) may be so determined that, if $r \neq s$ and $m_{rs} \neq 0$, $m_{rs} = 1$ and $m_{sr} = \epsilon$.*

LEMMA 4. *The matrix M in (20) may be obtained by a permutation of the rows and the same permutation of the columns from the diagonal block matrix*

$$[n_1, n_2, \cdots, n_f, N_1, N_2, \cdots, N_g] \tag{21}$$

where n_i is an element of K and

$$N_j = \begin{pmatrix} x_j & 1 \\ \epsilon & 0 \end{pmatrix}$$

and $x_j = 0$, if $\chi \neq 2$.

Let H be an arbitrary matrix satisfying (7) and A any square matrix. Let B and C be the matrices defined by (6) and let

$$BHB^* = R.$$

Then by (20)

$$LBHB^*L^* = M.$$

Further, since C in (6) is quasi-triangular and L is triangular, by lemma 1, the matrix

$$T = LCL^{-1}, \tag{22}$$

is quasi-triangular of the same type as C.

By (22) and (6),

$$T = LBAB^{-1}L^{-1},$$

so that, if $LB = P$,

$$PAP^{-1} = T \quad \text{and} \quad PHP^* = M. \tag{23}$$

Hence we have

THEOREM I. *If $H^* = \epsilon H$ and A is any square matrix there exists a non-singular matrix P such that (23) is true where M is given by (20) and T is a*

quasi-triangular matrix. The type of T is determined by the elementary factors of $A - xE$.

We have as a consequence of Lemma 3, the

COROLLARY. *The matrix M of Theorem I may be obtained by a permutation of the rows and the same permutation of the columns from the diagonal block matrix* (21).

While it is possible, except when $\chi = 2$, to reduce the matrices N_j to diagonal form, this reduction would in general destroy the quasi-triangular property of the matrix T.

3. Special cases. If the field K is algebraically closed then the matrix T is a triangular matrix. In particular, if K is the complex field and H is an hermitian matrix, each n_i may obviously be reduced to ± 1. Since the matrix N_j is not definite, if H is definite no matrices of the form N_j can occur in (21) while each n_i has the same value $+1$ or -1. Accordingly we have result I and in a similar manner, if K is the real field, we obtain the corresponding result about a definite real symmetric matrix H.

If the automorphism over K is of period one and $\epsilon = -1$, so that H is skew symmetric, in (21) each n_i is zero when $\chi \neq 2$. In particular if H is non-singular and therefore of even order $2m$, the matrix in (21) is obtained from the matrix $\begin{pmatrix} 0 & E_m \\ -E_m & 0 \end{pmatrix}$ by a permutation of the rows and columns. In case K is algebraically closed the same permutation applied to T yields a matrix X where, when $i \neq j$, $x_{ij}x_{ji} = 0$. We have therefore the following corollary: *If $G = \begin{pmatrix} 0 & E_m \\ -E_m & 0 \end{pmatrix}$ and A is any square matrix of order $2m$ over K where K is algebraically closed and $\chi \neq 2$, there exists a non-singular matrix P such that $PGP' = G$ and $PAP^{-1} = X = (x_{ij})$, where $x_{ij}x_{ji} = 0$ for all values of $i, j, i \neq j$.*

Results of a similar nature to the above may be deduced in other cases but are as a rule considerably more complicated.

THE JOHNS HOPKINS UNIVERSITY.

GENERALIZED STIRLING TRANSFORMS OF SEQUENCES.*

By E. T. Bell.

1. What are here (§ 5) called the Stirling transforms of a sequence arose as follows. If

$$\alpha_n, \beta_n \equiv T^{(n)}(\alpha_0, \cdots, \alpha_n), \qquad (n = 0, 1, \cdots)$$

are sequences of integers, or of functions which take integer values for integer values of their variables, what are possible choices for the functions $T^{(n)}$ so that, from congruence properties of the α_n, congruence properties can be inferred for the β_n? As congruence properties of sequences are referred ultimately to Fermat's theorem, which in turn follows from Lagrange's identical congruence

$$t(t-1)\cdots(t-p+1) \equiv t^p - t \bmod p, \tag{1.1}$$

p prime, the question may be sharpened by requiring the inference from the α_n to the β_n to be through (1.1). This leads directly to the generalized Stirling numbers (proved to be integers) defined in § 2, and to the transforms by means of them of any sequence as discussed in § 5. There are already generalizations of the Stirling numbers in use, but none is appropriate for the purpose described, and we devise another. Incidentally, this generalization unifies the ordinary Stirling numbers of both kinds, exhibiting them as the special cases $\zeta_s^{(n,1)}, \zeta_s^{(n,-1)}$, $n, s = 0, 1, \cdots$ of one triply infinite set of integers $\zeta_s^{(n,r)}$, $r = 0, \pm 1, \pm 2, \cdots$.

Applications of the general considerations developed here are immediate and so numerous that we reserve detailed examples to specific sequences for another occasion. The generalized Bernoulli and Euler functions of Lucas, Cesàro, Nörlund, and others, alone provide an inexhaustible store of results for the corresponding generalized numbers of Bernoulli, Euler, Genocchi, and Lucas, when to them are applied the very general results of § 6.

It is to be noted that although infinite processes with convergence essential have occasionally been used heuristically, their use is not necessary, and in all cases strictly finite proofs of the final results concerning Stirling transforms have either been given in full or sufficiently outlined. However, where suitable convergence conditions are satisfied, the heuristic formulas are both interesting and useful in applications.

* Received May 9, 1938.

Frequent use will be made of the following lemma, whose proof is obvious and may be omitted.

(1.2) If one of three functions $f(t), f(e^t-1), f(\log(1+t))$ has an absolutely convergent MacLaurin expansion for some $|t|>0$, then all three have.

It will be convenient to use the symbolic method, in which α is the umbra of the sequence α_n, $n=0,1,\cdots$, or of the vector $(\alpha_0,\alpha_1,\cdots)$, and $\alpha^n\equiv\alpha_n$. Umbral equality, $\alpha=\beta$, signifies $\alpha_n=\beta_n$, $n=0,1,\cdots$, and if $f(t)$ has the absolutely convergent expansion $\sum_0^\infty \alpha_n t^n/n!$, we write

$$f(t)=e^{\alpha t}=\exp \alpha t. \tag{1.3}$$

It follows that if

$$f(t)=e^{\alpha t},\ g(t)=e^{\beta t},\cdots,h(t)=e^{\gamma t},$$

then

$$f(t)g(t)\cdots h(t)=e^{\sigma t},$$

where $\sigma=\alpha+\beta+\cdots+\gamma$, that is,

$$\sigma^n\equiv\sigma_n=(\alpha+\beta+\cdots+\gamma)^n,$$

in which $\alpha^u\beta^v\cdots\gamma^w$, after formal expansion of the right by the multinomial theorem, is replaced by $\alpha_u\beta_v\cdots\gamma_w$. Note that exponents 0, 1, as in α^0,α^1, are treated precisely as any others $\geqq 0$, $\alpha^0=\alpha_0$, $\alpha^1=\alpha_1$; also,

$$(\alpha+\beta+\cdots+\gamma)^0=\alpha_0\beta_0\cdots\gamma_0.$$

Throughout the paper, the symbol $\delta_r{}^s$ is a Kronecker delta, $\delta_r{}^r=1$, $\delta_r{}^s=0$, $r\neq s$.

2. In (1.2) take $f(t)\equiv t^n$, n an integer >0. Denote by τ, $\equiv\tau^1$, the operator which transforms t^n into $(e^t-1)^n$, and by τ^{-1} the inverse of τ:

$$\tau t^n=(e^t-1)^n,\qquad \tau^{-1}t^n=[\log(1+t)]^n,\qquad \tau^0t^n=t^n. \tag{2.1}$$

Powers of τ are defined recursively, giving the iterations $\tau^u t^n$, $\tau^{-u}t^n$, u an integer $\geqq 0$:

$$\tau^u t^n=\tau(\tau^{u-1}\,t^n),\qquad \tau^{-u}t^n=\tau^{-1}(\tau^{-u+1}\,t^n). \tag{2.2}$$

If r,s are any integers, $\tau^r=\tau^s$ signifies $\tau^rt^n=\tau^st^n$. The iteration is commutative and associative. Hence τ generates an abelian group, $\mathbf{T}$, in which the composition (or "multiplication") is defined by postulating the equivalence of the statements

$$\tau^r(\tau^st^n)=\tau^{r+s}t^n,\qquad \tau^r\tau^s=\tau^{r+s}. \tag{2.3}$$

The identity in $\mathbf{T}$ is τ^0, and τ^r, τ^{-r} are inverses.

By (1.2), the functions

$$(2.4)\qquad \tau^r t^n \equiv f^{(n,r)}(t),\ n, r \text{ integers},\ n > 0,\ r \gtreqless 0,$$

have absolutely convergent MacLaurin series for some common $|t| > 0$ and all finite n, r. Hence, by (1.3), we may write

$$(2.5)\qquad f^{(n,r)}(t) = n!\exp[t\zeta^{(n,r)}] \equiv n!\sum_{s=0}^{\infty} \zeta_s^{(n,r)} t^s/s!,$$

thus defining the $\zeta_s^{(n,r)}$, $s = 0, 1, \cdots$, for integers $n > 0$ and arbitrary integers r. If now we write $\zeta_s^{(0,r)} \equiv \delta_s^0$, (2.5) holds also for $n = 0$.

If n, r are integers, $n \geqq 0$, $r \gtreqless 0$, we shall call $\zeta_s^{(n,r)}$, $s = 0, 1, \cdots$, the *generalized Stirling numbers* of *degree n, rank r*. The $\zeta_s^{(n,-1)}$, $\zeta_s^{(n,1)}$ are the ordinary Stirling numbers $S_s^{(n)}$, $\mathfrak{S}_s^{(n)}$ of the first, second kind respectively,

$$(2.6)\qquad [\log(1+t)]^n = n!\exp[S^{(n)}t], \qquad S_s^{(n)} = \zeta_s^{(n,-1)};$$

$$(2.7)\qquad (e^t - 1)^n = n!\exp[\mathfrak{S}^{(n)}t], \qquad \mathfrak{S}_s^{(n)} = \zeta_s^{(n,1)}.$$

Equivalent definitions of $S^{(n)}$, $\mathfrak{S}^{(n)}$ by means of factorial coefficients and differences of zero are

$$(2.8)\qquad (t)_0 \equiv 1, \qquad (t)_n \equiv \prod_{s=0}^{n-1}(t-s) = \sum_{s=1}^{n} S_n^{(s)} t^s, \qquad n > 0;$$

$$(2.9)\qquad s!\,\mathfrak{S}_n^{(s)} \equiv \Delta^s 0^n, \qquad t^n = \sum_{s=1}^{n} \mathfrak{S}_n^{(s)}(t)_s, \qquad n > 0;$$

$$(2.10)\qquad S_0^{(0)} = \mathfrak{S}_0^{(0)} = 1; \qquad S_n^{(s)} = \mathfrak{S}_n^{(s)} = 0, \qquad s > n,\ n \geqq 0.$$

The last is a special case of

$$(2.11)\qquad \zeta_s^{(n,r)} = 0, \qquad n > s,\ s \geqq 0.$$

3. From the definitions we have

$$(3.1)\qquad f^{(n,r)}(t) = [f^{(1,r)}(t)]^n,$$

$$(3.2)\qquad f^{(1,r+1)}(t) = \exp[f^{(1,r)}(t)] - 1.$$

To these we apply the elementary processes of the umbral calculus to find recurrences, etc., for the $\zeta_s^{(n,r)}$. If α, β, γ are umbrae, and

$$A(t) = e^{\alpha t}, \qquad B(t) = e^{\beta t}, \qquad C(t) = e^{\gamma t},$$

the equation $A(t)B(t) = C(t)$ implies and is implied by $\alpha + \beta = \gamma$, and the last is equivalent to either of

$$(\alpha+\beta)^n=\gamma^n, \qquad \sum_{s=0}^{n}\binom{n}{s}\alpha_{n-s}\beta_s=\gamma_n, \qquad (n=0,1,\cdots).$$

Also, if D_t is the operator d/dt,

$$D_t e^{\alpha t}=\alpha e^{\alpha t}=\sum_{s=0}^{\infty}\alpha_{s+1}t^s/s!.$$

As a special caution in operating with umbrae, note again that zero exponents must be treated precisely as any others. Thus, for example, the first term in the expansion of $(1+\alpha)^n$ is α^0, $=\alpha_0$, and not 1, unless $\alpha_0=1$. Reduction of

$$D_t f^{(n,r+1)}(t)=D_t[\exp\{f^{(1,r)}(t)\}-1]^n$$

by (3.2) gives

$$D_t f^{(n,r+1)}(t)=nf^{(n-1,r+1)}(t)[1+f^{(1,r+1)}(t)]D_t f^{(1,r)}(t),$$

and hence, by (2.5), on equating coefficients of t,

$$\zeta_{s+1}^{(n,r+1)}=\zeta^{(1,r)}[\{\zeta^{(1,r)}+\zeta^{(n-1,r+1)}\}^s+\{\zeta^{(1,r)}+\zeta^{(1,r+1)}+\zeta^{(n-1,r+1)}\}^s]. \tag{3.3}$$

The right of (3.3) may be written

$$\sum_{u=0}^{s}\binom{s}{u}\zeta_{u+1}^{(1,r)}[\zeta_{s-u}^{(n-1,r+1)}+\{\zeta^{(1,r+1)}+\zeta^{(n-1,r+1)}\}^{s-u}];$$

$$\{\zeta^{(1,r+1)}+\zeta^{(n-1,r+1)}\}^{s-u}=\sum_{v=0}^{s-u}\binom{s-u}{v}\zeta_v^{(1,r+1)}\zeta_{s-u-v}^{(n-1,r+1)}.$$

We verify (3.3) for $r=0$, this case giving a recurrence for $\mathfrak{S}^{(n)}$ which is readily obtainable directly. Since $\zeta_s^{(1,0)}=\delta_s^1$, (3.3) for $r=0$ becomes

$$\zeta_{s+1}^{(n,1)}=\zeta_s^{(n-1,1)}+[\zeta^{(1,1)}+\zeta^{(n-1,1)}]^s.$$

The first term in the expansion of the umbral binomial is $\zeta_0^{(1,1)}\zeta_s^{(n-1,1)}$, which vanishes, by (2.11). Since $\zeta_u^{(1,1)}=1$, $u>0$, we get

$$\zeta_{s+1}^{(n,1)}=[1+\zeta^{(n-1,1)}]^s,$$

and hence, by (2.7), the recurrence in question,

$$\mathfrak{S}_{s+1}^{(n)}=[1+\mathfrak{S}^{(n-1)}]^s. \tag{3.4}$$

From (3.1), (3.2) we have

$$f^{(n,r)}(t)=[\log\{1+f^{(1,r+1)}(t)\}]^n;$$

whence, proceeding as before, we find the inversion (3.5) of (3.3), valid for $n>0$:

$$(3.5)\qquad \zeta^{(n,r)}_{s+1} + \zeta^{(n,r)}[\zeta^{(n,r)} + \zeta^{(1,r+1)}]^s = \zeta^{(1,r+1)}[\zeta^{(1,r+1)} + \zeta^{(n-1,r)}]^s.$$

When the left of (3.5) is expanded there is but one term $\zeta^{(n,r)}_{s+1}$, since $\zeta^{(n,r)}_{s+1}\zeta_0^{(1,r+1)}$, contributed by the binomial, vanishes. For $r = -1$, (3.5) gives the known recurrence

$$(3.6)\qquad S^{(n)}_{s+1} + sS_s^{(n)} = S_s^{(n-1)}$$

for the Stirling numbers of the first kind.

The equivalent (3.7) of (2.3) is the addition theorem for the $\zeta^{(n,r)}$ with respect to the rank r,

$$(3.7)\qquad \zeta_v^{(n,r+s)} = \sum_{u=0}^{v} \zeta_u^{(n,r)}\zeta_v^{(u,s)}, \qquad (v = 0, 1, \cdots).$$

This result is of particular importance later.

The addition theorem with respect to the degree follows at once from

$$f^{(m,r)}(t)f^{(n,r)}(t) = f^{(m+n,r)}(t),$$

for m, n non-negative integers, and is

$$(3.8)\qquad (m+n)!\,\zeta_v^{(m+n,r)} = m!\,n!\,[\zeta^{(m,r)} + \zeta^{(n,r)}]^v.$$

From (3.7), (3.8) we get

$$(3.9)\qquad [\zeta^{(m,r+s)} + \zeta^{(n,r+s)}]^v = \sum_{u=0}^{v} [\zeta^{(m,r)} + \zeta^{(n,s)}]^u \zeta_v^{(u,s)}.$$

It follows from (3.7) by mathematical induction that the $\zeta_v^{(n,r)}$ are integers, on using the known results that the $S_s^{(n)}$, $\mathfrak{S}_s^{(n)}$ are integers, and (2.6), (2.7). Thus, taking $r = s = 1$ in (3.7), we see that $\zeta_u^{(n,2)}$ is an integer; $r = 2$, $s = 1$ then gives $\zeta_u^{(n,3)}$ an integer. Similarly for $\zeta_u^{(n,-r)}$, $r > 0$. Since $\mathfrak{S}_u^{(n)}$, $n \leqq u$, is an integer > 0, the induction shows that $\zeta_u^{(n,r)} > 0$ if $n \leqq u$, $r > 0$. To determine the sign of $\zeta_u^{(n,-r)}$, $r > 0$, write

$$\zeta_u^{(n,-r)} \equiv (-1)^{n+u}\beta_u^{(n,r)}, \qquad r > 0,$$

for the moment. It follows from (2.6), (2.8), (2.10) that $\beta^{(n,-1)} > 0$, $n \leqq u$; and by (3.7),

$$\beta_v^{(n,-r-s)} = \sum_{u=0}^{v} \beta_u^{(n,-r)}\beta_v^{(u,-s)}, \qquad r > 0,\ s > 0.$$

Hence, by mathematical induction,

$$\beta_v^{(n,-r)} > 0, \qquad v \geqq 0,\ r > 0,\ n \leqq v.$$

Summarizing the results in this paragraph and (2.5), (2.11), we have

(3.10) For all integers $n \geqq 0$, $r \gtreqless 0$, $s \geqq 0$ the $\zeta_s^{(n,r)}$ are integers, and

$$\begin{aligned}
&\zeta_s^{(n,r)} = 0,\ n > s; \qquad \zeta_s^{(0,r)} = \delta_s^0, \qquad \zeta_s^{(n,0)} = \delta_s^n;\\
&\zeta_s^{(n,r)} > 0, \qquad n \leqq s,\ r > 0;\\
&(-1)^{n+s}\zeta_s^{(n,-r)} > 0, \qquad n \leqq s,\ r > 0.
\end{aligned}$$

Some immediate consequences of (3.7) are important for the arithmetic of the transforms mentioned in § 1. For $r + s = 0$ we get

$$\sum_{u=0}^{v} \zeta_u^{(n,r)}\zeta_v^{(u,-r)} = \delta_v^n, \tag{3.11}$$

which, for $r = 1$, is a well known property of the ordinary Stirling numbers. In (3.7) replace r by $r + 1$, and take $s = -1$. Then

$$\zeta_v^{(n,r)} = \sum_{u=0}^{v} \zeta_u^{(n,r+1)}\zeta_v^{(u,-1)}. \tag{3.12}$$

The last leads to a useful transformation. If α is any umbra, we define the symbolic factorial $(\alpha)_v$ by

$$(\alpha)_0 \equiv \alpha_0; \qquad (\alpha)_v \equiv \prod_{s=0}^{v-1} (\alpha - s), \qquad v > 0, \tag{3.13}$$

in which (as always in the umbral calculus) α^r is to be replaced by α_r after the symbolic product is multiplied out. By (2.6), (2.8), (3.12) it follows that

$$(\zeta^{(n,r)})_0 = \delta_0^n, \qquad \zeta_s^{(n,r)} = (\zeta^{(n,r+1)})_s, \qquad s > 0. \tag{3.14}$$

This is the meaning of the symbolic formalism in the following transformation.

If t be replaced by $\log(1 + t)$ in

$$f^{(n,r+1)}(t) = n!\exp[t\zeta^{(n,r+1)}],$$

the left becomes $f^{(n,r)}(t)$, and we get

$$e^{t\zeta^{(n,r)}} = (1 + t)^{\zeta^{(n,r+1)}}, \tag{3.15}$$

from which (3.14) follows on equating coefficients of t^s. Note that $t \to \log(1 + t)$ transforms $e^{\alpha t}$ into $e^{(\alpha)t}$, where α is any umbra, and (α) is the umbra of $(\alpha)_n$, $n = 0, 1, \cdots$.

Obviously (3.14) is suitable for the application of Lagrange's (1.1); (3.14) is the fundamental relation for the congruence properties of the $\zeta^{(n,r)}$ and the Stirling transforms defined in § 5.

4. Before considering Stirling transforms we note two functional equations suggested by what precedes, and some of the simpler congruence properties of the generalized Stirling numbers immediately deducible from § 3.

(4.1) The only analytic solution of each of the equations

$$f(e^t-1)=f(t), \qquad f(\log(1+t)=f(t)$$

is $f(t)\equiv$ an arbitrary constant.

It will suffice, by (1.2), to prove this for the first equation, as the second is obtained from the first by $t\to\tau t$. If $f(t)\equiv e^{at}$ is a solution,

$$\sum_{u=0}^{\infty}\alpha_u\frac{t^u}{u!}=\sum_{n=0}^{\infty}\frac{\alpha_n}{n!}(e^t-1)^n=\sum_{n=0}^{\infty}\Big[\alpha_n\sum_{u=0}^{\infty}\zeta_u{}^{(n,1)}\frac{t^u}{u!}\Big];$$

$$\alpha_u=\sum_{n=0}^{u}\zeta_u{}^{(n,1)}\alpha_n, \qquad (u=0,1,\cdots).$$

These equations give $\alpha_0=\alpha_0$, $\alpha_u=0$, $u>0$. Hence $f(t)$ is the arbitrary constant α_0.

In the following congruences p is prime. We use the congruences for binomial coefficients,

$$\binom{p}{s}\equiv 0,\ 0<s<p; \qquad \binom{p}{0}\equiv\binom{p}{p}\equiv 1 \bmod p.$$

For $v=p$, (3.8) becomes

$$(m+n)!\,\zeta_p{}^{(m+n,r)}\equiv m!\,n!\,[\zeta_0{}^{(m,r)}\zeta_p{}^{(n,r)}+\zeta_p{}^{(m,r)}\zeta_0{}^{(n,r)}] \bmod p.$$

If $mn>0$, $\zeta_0{}^{(m,r)}=\zeta_0{}^{(n,r)}=0$; and if $(m+n)<p$, $(m+n)!$ is prime to p. Hence, after an obvious change in notation,

$$(4.2) \qquad \zeta_p{}^{(n,r)}\equiv 0 \bmod p,\ 1<n<p.$$

For $r=-1$, (4.2) is equivalent to the corresponding information given by (1.1).

Taking $s=p$ in (3.5) we find

$$\zeta_{p+1}^{(n,r)}+\zeta_1{}^{(n,r)}\zeta_p{}^{(1,r+1)}\equiv\zeta_{p+1}^{(1,r+1)}\zeta_0{}^{(n-1,r)}+\zeta_1{}^{(1,r+1)}\zeta_p{}^{(n-1,r)} \bmod p,$$

which it is convenient to separate into the cases $n>1$, $n=1$:

$$(4.3) \qquad \zeta_{p+1}^{(n,r)}\equiv\zeta_1{}^{(1,r+1)}\zeta_p{}^{(n-1,r)} \bmod p;$$

$$(4.4) \qquad \zeta_{p+1}^{(1,r)}+\zeta_p{}^{(1,r+1)}\equiv\zeta_{p+1}^{(1,r+1)} \bmod p.$$

From (4.2), (4.3),

$$(4.5) \qquad \zeta_{p+1}^{(n,r)}\equiv 0, \bmod p, \qquad 2<n<p+1.$$

For n not in the indicated range, it is necessary to have the congruence proper-

ties of the $\zeta_s^{(1,r)}$. These have been fully discussed elsewhere,[1] so we pass on to (3.14).

In the paper cited the extension (4.6) of (1.1) is proved, $(t)_n$ denoting the factorial function $(t)_0 = 1$, $(t)_n = t(t-1)\cdots(t-n+1)$, $n > 0$.

$$(t)_{mp+u} \equiv (t^p - t)^m (t)_u \bmod p. \tag{4.6}$$

As a further extension it is also proved that if

$$m = \sum_{j=0}^{u} m_j p^{u-j}$$

is the expression of m in the scale of p,

$$(t)_m \equiv (t)_{m_u} \prod_{j=0}^{u-1} [t^{p^{u-j}} - t^{p^{u-j-1}}]^{m_j} \bmod p. \tag{4.7}$$

It is shown also that if Δ is the symbol of finite differences (the increment of the variable being 1), and if the numbers $f(0)$, $\Delta^s f(0)/s!$, $s > 1$, are integers, then, if r is an integer $\geqq 0$,

$$(t^p - t)^r f(t) \equiv (t)_{rp} f(0) + \sum_{s=1} \frac{\Delta^s f(0)}{s!} (x)_{rp+s} \bmod p, \tag{4.8}$$

the summation continuing until all subsequent differences vanish. Thus if $f(t)$ is a polynomial in t the sum is finite.

Hence if there are symbolic factorial relations, of the same general kind as (3.14), for a given sequence, the congruence properties of the sequence can be investigated by means of (4.6)–(4.8). The $\zeta_s^{(n,r)}$ and the Stirling transforms defined in § 5 exhibit such relations, and it will be seen (§ 5) that *these are the only families of sequences* $\Sigma_s^{(n)}$ $(n, s = 0, 1, \cdots)$ *such that consecutive sequences* $\Sigma^{(n)}$, $\Sigma^{(n+1)}$ *of the set are related factorially,* $\Sigma_s^{(n)} = (\Sigma^{n+1})_s$. The identical congruences (4.6)–(4.8) are readily deducible from Lagrange's (1.1); in proving (4.7), (4.8), Fermat's theorem, a consequence of (1.1), is used. Thus the problem stated in § 1 is solved here through the group T of § 2, which generates the required factorial relations.

A few examples for the $\zeta^{(n,r)}$ will suffice. From (3.14), (4.6) we get

$$\zeta_{mp+u}^{(n,r)} \equiv [(\zeta^{(n,r+1)})^p - \zeta^{(n,r+1)}]^m (\zeta^{(n,r+1)})_u \bmod p, \tag{4.9}$$

in which, as always, all indicated rational operations are to be completed before exponents are lowered. For $m = u = 1$, (4.9) gives

$$\zeta_{p+1}^{(n,r+1)} - \zeta_{p+1}^{(n,r)} \equiv \zeta_2^{(n,r+1)} \bmod p,$$

---

[1] In a paper on iterated exponential integers, to appear in the *Annals of Mathematics.*

a simple difference congruence of the type considered in the paper cited, whose solution (4.10) is obtained in an obvious way,

$$(4.10)\qquad \zeta_{p+1}^{(n,r)} \equiv \delta_{p+1}^{n} + \sum_{s=1}^{r} \zeta_2^{(n,s)} \bmod p, \qquad r > 0,$$

$$\zeta_{p+1}^{(n,r)} \equiv \delta_{p+1}^{n} - \sum_{s=r+1}^{0} \zeta_2^{(n,-s)} \bmod p, \qquad r < 0.$$

For $r = -1$ in the second, $r = 1$ in the first, these give

$$(4.11)\qquad S_{p+1}^{(n)} \equiv \delta_{p+1}^{n} - \delta_2{}^{n}; \quad \mathfrak{S}_{p+1}^{(2)} \equiv 1, \quad \mathfrak{S}_{p+1}^{(m)} \equiv \delta_{p+1}^{(m)} \bmod p, \quad m > 2.$$

If $n > 2$ in (4.10) the sums vanish:

$$(4.112)\qquad \zeta_{p+1}^{(n,r)} \equiv \delta_{p+1}^{n} \bmod p, \qquad n > 2.$$

For $m = 2$, $u = 0$, (4.9) gives

$$\zeta_{2p}^{(n,r)} \equiv \zeta_{2p}^{(n,r+1)} - 2\zeta_{p+1}^{(n,r+1)} + \zeta_2{}^{(n,r+1)} \bmod p;$$

hence, by (4.112)

$$(4.12)\qquad \zeta_{2p}^{(n,r)} \equiv \delta_{2p}^{n} + 2r\delta_{p+1}^{n} \bmod p, \qquad n > 2.$$

For $r = -1, 1$ the last gives

$$(4.13)\qquad S_{2p}^{(n)} \equiv \delta_{2p}^{n} - 2\delta_{p+1}^{n}, \quad \mathfrak{S}_{2p}^{(n)} \equiv \delta_{2p}^{n} + 2\delta_{p+1}^{n} \bmod p, \qquad n > 2.$$

For $m = 1$, $u = 0$, (4.9) gives

$$(4.14)\qquad \zeta_p{}^{(n,r)} \equiv \delta_p{}^{n} \bmod p, \qquad n > 1;$$

and using this with the result of $m = p$, $u = 0$ in (4.9), we get

$$(4.15)\qquad \zeta_{p^2}{}^{(n,r)} \equiv \delta_{p^2}{}^{n} + r\delta_p{}^{n} \bmod p, \qquad n > 1,$$

with special cases for the ordinary Stirling numbers as before. Continuing thus, and using the other general congruences in this section, a detailed analysis of the congruence properties of the ordinary Stirling numbers for a prime modulus p (and for some forms of a composite modulus) may be given, precisely as was done in the paper cited for the iterated exponential integers. Similarly for the generalized Stirling numbers.

5. If r is a positive, zero, or negative integer, we define the *generalized Stirling transform* of *rank* r of any given sequence $\alpha_v{}^{(0)}$, $v = 0, 1, \cdots$, to be the sequence $\alpha_v{}^{(r)}$, $v = 0, 1, \cdots$, where

$$(5.1) \qquad \alpha_v^{(r)} \equiv \sum_{n=0}^{v} \zeta_v^{(n,r)} \alpha_n^{(0)}.$$

The range $v = 0, 1, \cdots$ *need not be indicated hereafter.*

It follows from (3.7) that if r, s are any integers,

$$(5.2) \qquad \alpha_v^{(r+s)} = \sum_{u=0}^{v} \zeta_v^{(u,s)} \alpha_u^{(r)} = \sum_{u=0}^{v} \zeta_v^{(u,r)} \alpha_u^{(s)}.$$

Taking $s = -1$ and replacing r by $r+1$ in (5.2), we get, by (2.8),

$$(5.3) \qquad \alpha_v^{(r)} = (\alpha^{(r+1)})_v.$$

Hence if $\alpha_v^{(0)}$ is a sequence of integers, the congruences (4.6)–(4.8) are applicable.

The unique part of generalized Stirling transforms in the solution of the problem of § 1 is seen from (5.3) and

(5.4) The general solution of the umbral equation $\xi = (\theta)$, that is, of $\xi_v = (\theta)_v$, $v = 0, 1, \cdots$, is $\xi \equiv \alpha^{(r)}$, $\theta \equiv \alpha^{(r+1)}$, where r is an arbitrary integer and $\alpha^{(0)}$ the umbra of an arbitrary sequence.

To prove (5.4) we have:

(5.5) If the integer r and the umbra γ are given, the umbral equation $\phi^{(r)} = \gamma$ has the unique solution $\phi^{(0)}$,

$$\phi_v^{(0)} \equiv \sum_{n=0}^{v} \zeta_v^{(n,-r)} \gamma_n.$$

That this is indeed a solution follows from (3.11), (5.1). For, from the definition (5.1) of the Stirling transform of rank r of any given sequence, and $\gamma = \phi^{(r)}$, we have

$$\gamma_v = \phi_v^{(r)} = \sum_{n=0}^{v} \zeta_v^{(n,r)} \phi_n^{(0)};$$

and therefore, on substituting for

$$\phi_n^{(0)}, = \sum_{s=0}^{n} \zeta_n^{(s,-r)} \gamma_s$$

from the assumed solution,

$$\gamma_v = \sum_{n=0}^{v} \zeta_v^{(n,r)} \sum_{s=0}^{n} \zeta_n^{(s,-r)} \gamma_s,$$

the right of which, by (3.11), is $\zeta_v^{(s,0)} \gamma_s$, $= \delta_s^v \gamma_s$, $= \gamma_v$. Reversing the steps of this verification, we thus prove that the stated $\phi^{(0)}$ is a solution of the given equation. The unicity is immediate by a simple contradiction from

(5.6) The only solution of $\phi^{(r)} = \phi^{(0)}$, $r \neq 0$, or of $\phi^{(r)} = \phi^{(s)}$, $r \neq s$, is $\phi_0^{(0)}$ an arbitrary constant, $\phi_n^{(0)} = 0$, $n > 0$.

This is proved as in (4.1). We now prove (5.4) by assuming, without loss of generality, by (5.5), that $\xi \equiv \alpha^{(r)}$. By (5.3), a value of θ is then $\theta \equiv \alpha^{(r+1)}$, and by an application of (5.6) and the obvious (5.7), the proof is complete:

(5.7) If ϵ is a given umbra, the unique solution of the umbral equation $(\psi) = (\epsilon)$, that is, of $(\phi)_v = (\epsilon)_v$, $v = 0, 1, \cdots$, is $\psi \equiv \epsilon$.

Defining the two statements

$$\alpha_v^{(r)} \times \alpha_v^{(s)} = \alpha_v^{(r+s)}, \qquad \alpha^{(r)} \times \alpha^{(s)} = \alpha^{(r+s)}$$

to be equivalent, we see by (5.2), (5.6) that with respect to the composition $\times$ the set $\alpha^{(n)}$, $n = 0, \pm 1, \pm 2, \cdots$ is an abelian group, in which $\alpha^{(0)}$ is the identity and $\alpha^{(n)}$, $\alpha^{(-n)}$ are inverses.

If $\alpha^{(0)}$ is such that $\exp(\alpha^{(0)}t)$ is absolutely convergent for some $|t| > 0$, (1.2), (2.4), (3.1) may be applied:

$$\exp[\alpha^{(0)} f^{(1,r)}(t)] = \exp[\alpha^{(r)} t]. \tag{5.8}$$

6. The results in this section are of a very general nature, and are applicable to any of the numerous families of Appell polynomials in the literature as special cases.

Let $\alpha, \beta, \cdots, \rho, \sigma$ be any umbrae such that $\sigma = \alpha + \beta + \cdots + \rho$, and hence

$$\sigma_n = (\alpha + \beta + \cdots + \rho)^n = \Sigma M^{(n)}_{a, b, \ldots, r} \alpha_a \beta_b \cdots \rho_r, \qquad n > 0,$$

where M is a multinomial coefficient. Assume (for a moment only) that $e^{t\alpha}, e^{t\beta}, \cdots, e^{t\rho}$, and hence also $e^{t\sigma}$, have a common domain $|t| > 0$ of absolute convergence. Let (α) denote the umbra of the sequence $(\alpha)_n$, $n = 0, 1, \cdots$ of symbolic factorials,

$$(\alpha)_0 \equiv \alpha_0, \qquad (\alpha)_r \equiv \prod_{s=0}^{r-1} (\alpha - s) \equiv \sum_{u=1}^{r} S_r^{(u)} \alpha_u, \qquad r > 0,$$

and similarly for $(\beta), \cdots, (\sigma)$. Since $\sigma = \alpha + \beta + \cdots + \rho$, we have

$$e^{\sigma t} = e^{\alpha t} e^{\beta t} \cdots e^{\rho t},$$

and hence, by $t \to \log(1 + t)$,

$$(1 + t)^\sigma = (1 + t)^\alpha (1 + t)^\beta \cdots (1 + t)^\rho;$$

that is,

$$e^{(\sigma)t} = e^{(\alpha)t}\, e^{(\beta)t} \cdots e^{(\rho)t},$$

and therefore

$$e^{(\sigma)t} = e^{[(\alpha)+(\beta)+\cdots+(\rho)]t}.$$

Hence (6.1), (6.2) are equivalent,

$$(6.1) \qquad \sigma = \alpha + \beta + \cdots + \rho,$$

$$(6.2) \qquad (\sigma)_n = [(\alpha) + (\beta) + \cdots + (\rho)]^n.$$

Expanding the right of (6.2) by the (symbolic) multinomial theorem, and the left by (2.8), we have

$$(6.3) \qquad (\sigma)_0 = (\alpha)_0(\beta)_0 \cdots (\rho)_0, \qquad \sigma_0 = \alpha_0\beta_0 \cdots \rho_0;$$

$$\sum_{u=1}^{n} S_n{}^{(u)}\sigma_u = \sum M^{(n)}_{a,b,\ldots,r}\,(\alpha)_a(\beta)_b \cdots (\rho)_r, \qquad n > 0.$$

Finally then, (6.1), (6.3) are equivalent.

The convergence restrictions necessary to validate the foregoing proof are irrelevant to the conclusion, which holds for any whatever umbrae $\alpha, \cdots, \sigma$. For, the equivalence of (6.1), (6.3) can be established directly by finite processes, as follows. Write $\beta + \cdots + \rho = \gamma$, so that $\sigma = \alpha + \gamma$; it is to be shown that $(\sigma)_n = [(\alpha) + (\gamma)]^n$. But this follows on comparing, first, coefficients of α_j in the assumed (finite) equality, and then, in the result, coefficients of γ_j. A known identity in ordinary Stirling numbers follows. The steps are reversible. Hence the proof is complete for σ a sum of two umbrae. By mathematical induction the general result follows immediately.

(6.3) If $\alpha, \beta, \cdots, \rho, \sigma$ are any umbrae such that (6.1) holds, then (6.2) holds, and conversely.

Write $\alpha \equiv \alpha^{(0)}, \cdots, \sigma \equiv \sigma^{(0)}$, and as before denote the Stirling transforms of rank v of $\alpha^{(0)}, \cdots, \sigma^{(0)}$ by $\alpha^{(v)}, \cdots, \sigma^{(v)}$ respectively. Then, obviously, the first of (6.4) implies the second,

$$(6.4) \qquad \sigma^{(0)} = \alpha^{(0)} + \beta^{(0)} + \cdots + \rho^{(0)}, \quad \sigma^{(v)} = \alpha^{(v)} + \beta^{(v)} + \cdots + \rho^{(v)}.$$

By (6.3), $\alpha^{(0)}, \cdots, \sigma^{(0)}$ may be replaced by $\alpha^{(v)}, \cdots, \sigma^{(v)}$ respectively in (6.2). Hence (6.5), (6.6) are equivalent:

$$(6.5) \qquad \sigma^{(0)} = \alpha^{(0)} + \beta^{(0)} + \cdots + \rho^{(0)};$$

$$(6.6) \qquad (\sigma^{(v)})_n = [(\alpha^{(v)}) + (\beta^{(v)}) + \cdots + (\rho^{(v)})]^n,$$
$$(v = 0, \pm 1, \pm 2, \cdots, n = 0, 1, \cdots).$$

It follows by (2.8), (5.3) that (6.5) and (6.7), also (6.5) and (6.8), are equivalent:

(6.7) $$(\sigma^{(v)})_n = \sum M^{(n)}_{a,b,\ldots,r}\,\alpha_a{}^{(v-1)}\beta_b{}^{(v-1)}\cdots\rho_r{}^{(v-1)};$$

(6.8) $$\sum_{s=1}^{n} S_n{}^{(s)}\sigma_s{}^{(v)} = \sum M^{(n)}_{a,b,\ldots,r}\,\alpha_a{}^{(v-1)}\beta_b{}^{(v-1)}\cdots\rho_r{}^{(v-1)},$$

for v, n as in (6.6).

In the umbral calculus, umbral derivation, D_ξ, is defined as follows. If ξ is any umbra,

$$D_\xi \xi_n \equiv n\xi_{n-1}, \qquad (n = 0, 1, \cdots),$$

where ξ_{-1} is defined to be identically zero. If ξ is a particular one of $\alpha, \beta, \cdots, \rho$,

(6.9) $$D_\xi(\alpha+\beta+\cdots+\rho)^n = n(\alpha+\beta+\cdots+\rho)^{n-1}.$$

It follows from (6.6) that if $\xi^{(v)}$ is a particular one of $\alpha^{(v)}, \cdots, \rho^{(v)}$,

(6.10) $$D_{\xi^{(v)}}(\sigma^{(v)})_n = n(\sigma^{(v)})_{n-1},$$

in which we recognize a generalization of the characteristic property of Appell polynomials.

A further consequence of (6.3) is immediate, for we may replace $\alpha^{(0)}, \beta^{(0)}, \cdots, \rho^{(0)}$ by their Stirling transforms of any ranks $u, v, \cdots, w$. Thus (6.11) implies, but is not equivalent to, (6.12):

(6.11) $$\sigma = \alpha^{(u)} + \beta^{(v)} + \cdots + \rho^{(w)};$$

(6.12) $$(\sigma)_n = [(\alpha^{(u)}) + (\beta^{(v)}) + \cdots + (\rho^{(w)})]^n.$$

Hence (6.11) implies

(6.13) $$\sum_{h=1}^{n} S_n{}^{(h)}\sigma_h = \sum M^{(n)}_{a,b,\ldots,r}\,\alpha_a{}^{(u-1)}\beta_b{}^{(v-1)}\cdots\rho_c{}^{(w-1)};$$

and if ξ denotes a particular one of $\alpha^{(u)}, \beta^{(v)}, \cdots, \rho^{(w)}$,

(6.14) $$D_\xi(\sigma)_n = n(\sigma)_{n-1}.$$

The results for ordinary Appell polynomials $(x+\alpha)^n$, x an ordinary variable, α an umbra, are included in the foregoing, when x is interpreted as the umbra of the sequence $x^0, x^1, x^2, \cdots$ of the non-negative powers x^n $(n = 0, 1, \cdots)$ of the ordinary variable x.

In arithmetical applications of this section, the congruence properties of multinomial coefficients and the extensions of (1.1) in § 4 are used.

CALIFORNIA INSTITUTE OF TECHNOLOGY.

AN ENUMERATION OF THE GROUPS OF ORDER *pqrs*.*

By D. T. Sigley.

1. Introduction. The number of abstract groups of an order which is the product of less than four distinct prime factors has been determined and enumerated, wholly or in part, by many writers including Cayley,[1] Netto,[2] Cole and Glover,[3] Burnside,[4] Hölder,[5] and Miller.[6,7] A more complete history of the problem may be obtained from two papers by Miller [8] under the titles "*Report on the recent progress in the theory of groups of finite order*" and "*Historical note on the determination of abstract groups of a given order.*" The structure of the groups whose order is the product of distinct prime numbers is known.[5] The number of distinct abstract groups of an order which is the product of distinct prime numbers and which involves fewer than four unity congruences has been enumerated.[7] The object of this paper is to enumerate the distinct abstract groups of an order, *pqrs*, which is the product of four distinct prime factors. The number of unity congruences[7] involved in the order has been used as a basis for the classification of the cases which arise in this determination.

2. Unity congruence relations on four prime factors. Let G represent any finite abstract group of order $g = pqrs$, where p, q, r, and s are distinct prime numbers in order of decreasing magnitude. We shall determine the number of distinct abstract groups of order g. The number of abstract groups of order g is a function of the number of unity congruences involved in g. The maximum number of unity congruences on the four prime factors of g is six. If we represent the unity congruence relation $p \equiv 1$, mod q, by $p(q)$,

* Received February 24, 1938.

[1] Cayley, *Philosophical Magazine*, vol. 13 (1854).

[2] Netto, *Substitutionentheorie*, 1892, pp. 133-137.

[3] Cole and Glover, *American Journal of Mathematics*, vol. 15 (1893), pp. 193-194.

[4] Burnside, *Theory of Groups*, 1896, pp. 26, 100.

[5] Hölder, *Mathematische Annalen*, vol. 43 (1893), and *Mathematische Annalen*, vol. 46 (1895).

[6] Miller, *Proceedings of the National Academy of Sciences*, vol. 18 (1932), two papers.

[7] Miller, *American Journal of Mathematics*, vol. 55 (1933), pp. 22-28.

[8] Miller, *Bulletin of the American Mathematical Society*, vol. 5 (1899), pp. 227-249; or *Collected Works*, vol. 1 (1935), pp. 326-344; Miller, *Collected Works*, pp. 91-98.

then the possible unity congruences involved in g are: $p(q)$, $p(r)$, $p(s)$, $q(r)$, $q(s)$, and $r(s)$. The number of groups of order g for which g involves less than four unity congruences is known. Hence, in order to complete the enumeration, it is necessary to consider only those cases in which g involves four, five, or six unity congruences. Combinations of four unity congruences may be selected from six unity congruences in fifteen ways, which give rise to fifteen distinct cases to consider. Correspondingly, there are six cases to consider when the number of unity congruences involved in g is five, and a single case to consider when this number is six.

From Number Theory it follows that there exists a number of the form $pqrs$, which involves any given one of the 64 possible combinations of unity congruences on the primes p, q, r, and s.

3. General method of enumeration. The groups of order $pqrs$, which involves any given set of unity congruences, may be enumerated by classifying them according to the order of the central. The central must necessarily be of an order of the *form* g, pq, p, or 1. If we let $N_{p_1p_2p_3\ldots p_k}$ represent the number of distinct abstract groups of an order $p_1p_2p_3\cdots p_k$, where the p's are distinct prime numbers, in which the central is the identity, then the number N of groups of order g may be written as

$$(1)\qquad N = 1 + N_{pq} + N_{pr} + N_{ps} + N_{qr} + N_{qs} + N_{rs} + N_{pqr} + N_{pqs} + N_{prs} + N_{qrs} + N_{pqrs}.$$

Thus we see that the enumeration of the groups of an order which is the product of distinct prime factors may be made to depend upon the enumeration of the groups of this order, and similar orders with fewer prime factors, in which the central is the identity.

The values of all of the symbols in the right member of (1), except the last, are known. Thus, $N_{pq} = 1$, or 0 according as $p(q)$, or not. Also, $N_{pqr} = r$, $r - 1$, 1, or 0, according as the three primes p, q, and r satisfy the unity congruence relations $p(q)$, $p(r)$, and $q(r)$; $p(r)$, and $q(r)$; $p(q)$, and $p(r)$; or any other possible combination.

4. The enumeration of the groups of order g in which the central is the identity. To find the numerical value of N_{pqrs}, that is, to find the number of distinct abstract groups of order g in which the central is the identity, we classify these groups according to the order of the commutator subgroup in each group. This commutator subgroup may be of order p, pq, pr, or pqr. We shall now state three theorems which will be sufficient for the enumeration of the groups of order g for each of these cases.

THEOREM 1. *The number of distinct abstract groups of order* $g = \prod_{i=1}^{k} p_i$, *where* p_i, $i = 1, 2, 3, \cdots, k$, *are distinct prime numbers in the order of decreasing magnitude, which have a central of order* 1 *and a commutator subgroup of prime order is one or zero according as* $p_1(p_i)$, *for every* $i = 2, 3, \cdots, k$, or not.

The theorem follows easily from known results.

THEOREM 2. *The number of distinct abstract groups of order* $g = \prod_{i=1}^{k} p_i$, *where the p's are distinct primes in the order of decreasing magnitude, whose generators* P_i, $i = 1, 2, \cdots, k$, *fulfil the abstract defining relations*

$$P_i^{p_i} = 1, \qquad (i = 1, 2, \cdots, k),$$
$$P_k^{-1} P_i P_k = P_i^{\alpha_i}, \qquad (i = 1, 2, \cdots, k-1),$$

and $\alpha_i \not\equiv 1, \mod p_i$, *is* $(p_k - 1)^{k-2}$.

This theorem may be proved as follows. Let H represent the invariant subgroup of G generated by $P_1, P_2, \cdots, P_{k-1}$. H is a cyclic group since a prime factor of the order h of H is congruent to unity with respect to another such prime factor. The operator P_k can transform the subgroup H into itself in $(p_k - 1)^{k-1}$ ways in which the central of G is the identity, because of the relations

$$P_k^{-1} P_i P_k = P_i^{\alpha_i}, \ i = 1, 2, \cdots, k-1, \qquad \alpha_i \not\equiv 1, \mod p_i.$$
$$P_k^{-p_k} P_i P_k^{p_k} = P_i^{\alpha_i^{p_k}} = P_i,$$

whence

$$\alpha_i^{p_k} \equiv 1, \mod p_i,$$

which is satisfied by $p_k - 1$ distinct values of α_i less than p_i. The choice of P_k and α_i, $i = 1, 2, \cdots, k-1$, uniquely determines G. Therefore, the number of groups of order g is $(p_k - 1)^{k-1}$. But not all of these groups are distinct since they fall into sets of simply isomorphic groups, each set containing the $p_k - 1$ groups which are obtained when the $p_k - 1$ co-sets of a particular group G with respect to H are permuted cyclically. Hence, the number of distinct abstract groups whose generators fulfil the abstract defining relations of the theorem is $(p_k - 1)^{k-1}$.

THEOREM 3. *The number of distinct abstract groups* G *of an order* $g = pqrs$, *whose generators fulfil the abstract defining relations*

$$P^p = Q^q = R^r = S^s = 1,$$
$$R^{-1}PR = P^{\alpha_1}, \quad S^{-1}PS = P^{\alpha_2},$$
$$R^{-1}QR = Q^{\delta_1}, \quad S^{-1}QS = Q^{\delta_2},$$

where p, q, r, and s are distinct prime numbers and, where the α's are not congruent to unity, mod p, *and the δ's are not congruent to unity,* mod q, *is* $(r-1)(s-1)$.

Let H and K represent the invariant subgroups of indices rs, and s, respectively, in G. K may be obtained by adjoining to the cyclic subgroup H an operator of order r which transforms H into itself, and such that the central of K is the identity. By theorem 2, there are $(r-1)$ distinct abstract groups, K. G may be generated by adjoining to K an operator S, of order s, which transforms K into itself by transforming R into itself, and transforming the subgroup H into itself by transforming each of its generators into a power of itself different from the first power. These isomorphisms may be established in $(s-1)^2$ ways. Hence, the total number of groups is $(r-1)(s-1)^2$, which fall into sets of simply isomorphic groups, each set containing $s-1$ groups. The $s-1$ simply isomorphic groups in each set are those which may be obtained from a given G by permuting the co-sets of G with respect to K, cyclically. Hence the number of distinct abstract groups whose generators fulfil the given generating conditions is $(s-1)(r-1)$.

5. Results of the enumeration. The groups of order $pqrs$ have been enumerated by the method outlined in section 3, above, and by the applications of the theorems in section 4, for all of the possible cases which arise due to the various combinations of unity congruences which may exist in this order. The results are given in the following table. The groups are of odd order in all cases, except those in which $p(s)$, $q(s)$, and $r(s)$. In these latter cases, the groups will be of even order if $s=2$, and of odd order if s is an odd prime number.

Number of Groups of Order $pqrs$.

Congruence relations in $pqrs$.	Number of groups of order $pqrs$.
No unity congruence	1
One unity congruence	2
Two unity congruences (of the form)	
$p(q)$ $p(r)$	4
$p(q)$ $q(r)$	3
$p(q)$ $r(s)$	4
$p(r)$ $q(r)$	$r+2$
Three Unity congruences (three factors)	
$p(q)$ $p(r)$ $q(r)$ (typical)	$r+4$
(four factors)	
$p(q)$ $p(r)$ $p(s)$	8
$p(q)$ $p(r)$ $q(s)$ or $r(s)$	6
$p(q)$ $q(r)$ $q(s)$ or $r(s)$	5
$p(q)$ $q(r)$ $r(s)$	$r+3$
$p(s)$ $q(s)$ $r(s)$	s^2+s+2.

congruences [9]	central comm. subgr.	g	p_ip_j	p_i	1 p	pq	pr	pqr	
$q(s)r(s)$		1	4	$r+2$	1	r	0	0	$2r+8$
$q(r)r(s)$		1	4	$s+2$	1	s	0	0	$2s+8$
$p(r)q(s)$		1	4	$s+2$	1	0	s	0	$2s+8$
$p(s)r(s)$		1	4	$r+1$	0	r	0	0	$2r+6$
$p(s)q(s)$		1	4	r	0	0	1	0	$r+6$
$p(s)q(r)$		1	4	s	0	1	1	0	$s+7$
$p(r)r(s)$		1	4	$s+1$	0	s	0	0	$2s+6$
$p(r)q(s)$		1	4	s	0	1	s	0	$2s+6$
$p(r)p(s)$		1	4	s	0	0	1	0	$s+6$
$p(q)r(s)$		1	4	$r+s$	0	$rs+r+s-1$	0	0	$rs+2r+2s+4$
$p(q)p(s)$ $p(q)q(s)$		1	4	$r+s-1$	0	r	0	0	$2r+s+4$
$p(q)p(r)$ $p(q)q(r)$ $p(r)q(r)$		1	4	$3s-2$	0	s	0	$(s-1)^2$	s^2+2s+4
$r(s)$		1	5	$r+s+2$	1	$rs+r+s-1$	0	0	$rs+2r+2s+8$
$q(s)$		1	5	$r+s+1$	1	r	s	0	$2r+2s+8$
$q(r)$		1	5	$3s$	1	s	s	$(s-1)^2$	s^2+3s+8
$p(s)$		1	5	$r+s$	0	r	1	0	$2r+s+7$
$p(r)$		1	5	$3s-1$	0	s	s	$(s-1)^2$	s^2+3s+6
$p(q)$		1	5	$3s+r-2$	0	$rs+r+s-1$	0	$(s-1)^2$	$s^2+rs+2r+2s+$ [illegible]
		1	6	$3s+r$	1	$rs+r+s-1$	s	$(s-1)^2$	$s^2+rs+2r+3s+$ [illegible]

Kansas State College.

[9] All of the unity congruences $p(q)$, $p(r)$, $p(s)$, $q(r)$, $q(s)$, and $r(s)$ are present in the order $pqrs$ except those listed in this column.

THE RESOLUTION OF SINGULARITIES OF AN ALGEBRAIC CURVE.*

By H. T. MUHLY and O. ZARISKI.

Introduction. The object of this note is to give new and brief proofs of the following well known theorems concerning the resolution of the singularities of an algebraic curve:

1. *Every algebraic curve is birationally equivalent to an hyperspace curve which is free from singularities, both at finite distance and at infinity.*

2. *Any curve free from singularities in an hyperspace can be projected into a curve in the projective* 3*-space which is also free from singularities.*

3. *Every algebraic curve can be birationally transformed into a curve in the projective plane whose only singularities are ordinary double points.*

We assume that the underlying field of constants, K, is algebraically closed. From the classical theory of algebraic functions of one variable (be it function-theoretic or arithmetic) we use the notion of the Riemann surface of a field of such functions, the existence of a uniformizing parameter at a point of the Riemann surface, and the notion of the order of a function at a point (place).[1]

1. Let Σ be a field of algebraic functions of one variable. Any set of elements $\omega_1, \omega_2, \cdots, \omega_m$ in the field having the property that any element in Σ can be expressed as a rational function of them, defines a curve C in the projective m-dimensional space, S_m; $(\omega_1, \omega_2, \cdots, \omega_m)$ is the generic point of C. Clearly, Σ is the field of rational functions on C. We shall denote the curve C by the symbol $\{\omega_1, \omega_2, \cdots, \omega_m\}$.

A point $P(a_1, a_2, \cdots, a_m)$ of a curve C will be called a *simple point* of C if (a) P corresponds to only one point (place) of the Riemann surface Σ, and if (b) at least one of the elements $\omega_i - a_i$ vainshes to the order one at P (i. e., at the corresponding place). If P is at infinity, and if, for instance, the ratios $\omega_2/\omega_1, \omega_3/\omega_1, \cdots, \omega_m/\omega_1$ are finite and equal to $c_2, c_3, \cdots, c_m$ respectively at P (in which case ω_1 is necessarily infinite at P), then instead of (b) we require that one of the elements $1/\omega_1, \omega_i/\omega_2 - c_i$ vanish to the order one at P.

* Received September 19, 1938.

[1] R. Dedekind and H. Weber, "Theorie der algebraischen Funktionen einer Veränderlichen," *Journal für reine und angewandte Mathematik*, vol. 92 (1882).

It is evident that this definition of a simple point is invariant with respect to projective transformations in S_m.

If $\mathfrak{O}$ is the integral closure of the ring $K[\omega_1, \omega_2, \cdots, \omega_m]$ then an equivalent definition of a simple point at finite distance may be formulated as follows: P is a simple point of C if and only if the ideal $\mathfrak{P} = \mathfrak{O} \cdot (\omega_1 - a_1, \omega_2 - a_2, \cdots, \omega_m - a_m)$ is prime. Namely, if there existed two places P_1, P_2 on the Riemann surface of Σ at which $\omega_i = a_i$, $i = 1, 2, \cdots, m$, then there would exist in $\mathfrak{O}$ two prime ideals $\mathfrak{P}_1$, $\mathfrak{P}_2$ such that $\omega_i \equiv a_i(\mathfrak{P}_1)$ and $\omega_i \equiv a_i(\mathfrak{P}_2)$, in contradiction with the hypothesis that $\mathfrak{O} \cdot (\omega_1 - a_1, \cdots, \omega_m - a_m)$ is prime. Moreover, for at least one of the elements $\omega_i - a_i$, say for $\omega_1 - a_1$, we must have $\omega_1 - a_1 \not\equiv 0(\mathfrak{P}^2)$, and hence $\omega_1 - a_1$ vanishes to the order one at the corresponding place.

By a theorem of F. K. Schmidt [2] an independent variable x may be chosen in such a manner that Σ is a separable extension of $K(x)$. Let $\mathfrak{O}$ be the ring of integral functions of x in Σ, and let $\omega_1, \omega_2, \cdots, \omega_n$ be an integral base over $K[x]$ of the ring $\mathfrak{O}$, where n is the relative degree $[\Sigma : k(x)]$. *The curve* $\Gamma \equiv \{x, \omega_1, \omega_2, \cdots, \omega_n\}$ *in* S_{n+1} *is free from singularities at finite distances.* In view of the above ideal theoretic definition of a simple point, our assertion follows from the fact that since $\omega_1, \omega_2, \cdots, \omega_n$ is an integral base of $\mathfrak{O}$, the ring $K[x, \omega_1, \cdots, \omega_n]$ coincides with $\mathfrak{O}$ and hence is integrally closed.

We may assume that x becomes infinite to the order one at n distinct points of the Riemann surface of Σ. (Otherwise we use $x' = 1/(x - c)$ as the independent variable, where c is a constant such that $x - c$ vanishes to the order one at n distinct points of the Riemann surface). Let $P_1, P_2, \cdots, P_n$ be the points of the Riemann surface where x becomes infinite, and let ρ_i be a function in Σ which becomes infinite to the order one at P_i, and is finite at P_j, $j \neq i$. Every element in Σ can be put in the form $\xi/h(x)$, where $\xi \subset \mathfrak{O}$ and $h(x)$ is a polynomial in x. Hence we can find a polynomial $b(x)$ such that $b\rho_i$ is an integral function of x, $i = 1, 2, \cdots, n$. We consider the functions $\eta_1, \eta_2, \cdots, \eta_n$ defined as follows:

$$\eta_j = x^\lambda b(x)\rho_j \qquad (j = 1, 2, \cdots, n),$$

where λ is an integer which is taken so large that each η_j becomes infinite at every point P to an order higher than that of any of the functions ω_i. By construction, the function η_i is infinite to the order say m at P_j, $j \neq i$, and is infinite to the order $m + 1$ at P_i (m independent of i). Since η_i is an integral function of x, it is finite elsewhere.

[2] F. K. Schmidt, "Analytische Zahlentheorie in Körpern der Charakteristik p," *Mathematische Zeitschrift*, vol. 33 (1931).

The curve $\Gamma' \equiv \{x, \omega_1, \cdots, \omega_n; \eta_1, \cdots, \eta_n\}$ *in* S_{2n+1} *is free from singularities both at finite distance and at infinity.* Since the curve Γ was free from singularities at finite distance, the curve Γ' necessarily shares this property with Γ. The points at infinity on Γ' correspond to the points $P_1, P_2, \cdots, P_n$ of the Riemann surface. At P_i the quotients $1/\eta_i$, x/η_i, ω_j/η_i, and η_l/η_i, $l \neq i$, are all zero. Thus P_i gives rise to the point at infinity on the axis η_i. Moreover, at P_i η_j/η_i vanishes to the order one if $j \neq i$. Thus we have proved Theorem 1.

2. Let $C \equiv \{\omega_1, \omega_2, \cdots, \omega_m\}$ be a curve in the projective space $S_m(y_0, y_1, \cdots, y_m)$. On C we will have

$$y_0 : y_1 : \cdots : y_m = 1 : \omega_1 : \omega_2 : \cdots : \omega_m,$$

or introducing a factor of proportionality,

$$y_0 : y_1 : \cdots : y_m = \lambda_0 : \lambda_1 : \cdots : \lambda_m,$$

where $\lambda_i/\lambda_0 = \omega_i \subset \Sigma$. We shall also use the symbol $\{\lambda_0, \lambda_1, \cdots, \lambda_m\}$ to denote C.

Let $\omega'_i = \sum_{j=1}^{m} u_{ij}\omega_j$, $i = 1, 2$, where the u_{ij} are indeterminates. The elements ω'_1 and ω'_2 are connected by an irreducible equation

$$F(\omega'_1, \omega'_2; u_{ij}) = 0.$$

By formal partial differentiation, we obtain the relations

$$\begin{aligned} \omega_j F'_{\omega'_1} + F'_{u_{1j}} &= 0, \\ \omega_j F'_{\omega'_2} + F'_{u_{2j}} &= 0, \end{aligned} \qquad (j = 1, \cdots, n)$$

from which we conclude that if either $F'_{\omega'_1}$ or $F'_{\omega'_2}$ is different from zero, then any element of Σ can be expressed as a rational function of ω'_1 and ω'_2. The functions $F'_{\omega'_1}$, $F'_{\omega'_2}$ cannot both be zero, for if they were then also $F'_{u_{1j}} = F'_{u_{2j}} = 0$, $j = 1, \cdots, n$, and therefore we would have

$$F(\omega'_1, \omega'_2; u_{ij}) = [\phi(\omega'_1, \omega'_2; u_{ij})]^p,$$

where p is the characteristic of K.[3] Moreover, if the u's are selected so that say $F'_{\omega'_2} \neq 0$, then the polynomial $F(\omega'_1, \omega'_2; u_{ij})$ is not a polynomial in ω'^p_2, so that Σ is a separable extension of $K(\omega'_1)$.

Let $A_1, A_2, \cdots, A_k$ be the points of the Riemann surface at which not all ω_i are finite. If

[3] See for example B. L. van der Waerden, *Moderne Algebra*, vol. I, Chapter V.

$$\xi_i = \frac{c_{i0} + c_{i1}\omega_1 + \cdots + c_{im}\omega_m}{c_{00} + c_{01}\omega_1 + \cdots + c_{0m}\omega_m}, \qquad (i = 1, 2, \cdots, m)$$

then by a sufficiently general choice of the constants c we may be certain that each ξ_i is finite at all of the points A_j. Moreover, if we choose c_{00} so that the function $c_{00} + c_{01}\omega_1 + \cdots + c_{0m}\omega_m$ vanishes to the order one at say ν distinct points of the Riemann surface, and c_{i0} so that $c_{i0} + c_{i1}\omega_1 + \cdots + c_{im}\omega_m$ is different from zero at these points, it follows that the functions ξ_i all become infinite to the order one at the same points of the Riemann surface.

In S_m we make the coördinate transformation $T(c_{ij})$:

$$y'_i = \sum_{j=0}^{m} c_{ij} y_j, \qquad (i = 0, 1, \cdots, m).$$

The curve C is represented in the y' coördinate system by $\{\lambda'_0, \lambda'_1, \cdots, \lambda'_m\}$, where

$$\lambda'_i = \sum_{j=0}^{m} c_{ij} \lambda_j$$

and $\lambda'_i/\lambda'_0 = \xi_i \subset \Sigma$.

Obviously, the constants c_{ij} may be chosen so that ξ_2 is a primitive element of Σ over $K(\xi_1)$. Thus we can always obtain a representation $\{\xi_1, \xi_2, \cdots, \xi_m\}$ of a given curve C satisfying the three conditions: (1) Σ *is a separable extension of* $K(\xi_1)$,[4] (2) ξ_2 *is a primitive element of* $\Sigma/K(\xi_1)$, (3) *all of the* ξ *become infinite to the order one at the same* ν *points of the Riemann surface, and are finite elsewhere,* ν *being the relative degree* $[\Sigma : K(\xi_1)]$.

3. Let $\Gamma \equiv \{\xi_1, \cdots, \xi_m\}$ be any curve in S_m free from singularities. We assume that $\xi_1, \cdots, \xi_m$ satisfy conditions (1), (2), (3) of the preceding section. A point P of the Riemann surface of Σ will be called a branch point for the function ξ, if when $\xi = a$ at P, $\xi - a$ vanishes to an order larger than one; or if ξ has a pole of order greater than one at P. Let the set $\mathfrak{A} = (A_1, A_2, \cdots, A_\lambda)$ be the set of the common branch points for ξ_1 and ξ_2. A branch point for ξ_1 gives rise to a zero of $\Delta(\xi_1)$ the field discriminant of $\Sigma/K(\xi_1)$. Since Σ is a separable extension of $K(\xi_1)$, $\Delta(\xi_1)$ has only a finite number of zeros, so that the set $\mathfrak{A}$ contains only a finite number of points.

Let the set of points $\mathfrak{B} = (B_1, B_2, \cdots, B_\mu)$ be defined as follows: A point P of the Riemann surface of Σ is in $\mathfrak{B}$ if and only if there exists a second point $P' \neq P$ such that both ξ_1 and ξ_2 have the same finite values at P' as at P. Since ξ_2 is a primitive element of Σ, the equation

---

[4] A somewhat stronger result than condition (1) has recently been proved by B. L. van der Waerden, "Zur algebraischen Geometrie," *Mathematische Annalen*, vol. 115 (1938).

$$f(\xi_1, \xi_2) = 0,$$

of degree ν, connecting ξ_1 and ξ_2 is irreducible, so that its discriminant $D(\xi_1)$ is not identically zero. Any point of $\mathfrak{B}$ gives rise to a zero of $D(\xi_1)$, and hence $\mathfrak{B}$ can contain only a finite number of points.

Let $\mathfrak{C} = (C_1, C_2, \cdots, C_\nu)$ be the set of points on the Riemann surface of Σ at which ξ_1 becomes infinite.

Since a point A_i corresponds to a simple point on Γ it follows that if τ_i is a uniformizing parameter on A_i and if

$$\xi_j = c_{ji} + d_{ji}\tau_i + \cdots$$

is the expansion of ξ_j at A_i, then for a given i not all of the constants d_{ji} are zero. Since by hypothesis, $d_{1i} = d_{2i} = 0$, it follows that the linear form in $u_3, \cdots, u_m$

$$\psi_i(u) = \sum_{i=3}^{m} d_{ji}u_j \qquad (i = 1, 2, \cdots, \lambda)$$

is not identically zero.

Similarly, if k_{ji} is the value of ξ_j at B_i, and if B_a and $B_{a'}$ are a pair of points in $\mathfrak{B}$ such that $\xi_1 = a_1$, $\xi_2 = a_2$ at both B_a and $B_{a'}$, then the linear form

$$\phi_{aa'}(u) = \sum_{j=3}^{m} (k_{ja} - k_{ja'})u_j$$

is not identically zero.

Since all ξ_i are infinite to the order one at C_j, $1/\xi_1$ is a uniformizing parameter at C_j, and the ratios ξ_i/ξ_1 are all finite at C_j. Let $\xi_i/\xi_1 = l_{ij}$ at C_j, and let

$$\theta_{a\beta}(u) = \sum_{j=3}^{m} (l_{ja} - l_{j\beta})u_j.$$

Then if C_a and C_β are a pair of points in $\mathfrak{C}$ at which $l_{2a} = l_{2\beta}$ the corresponding $\theta_{a\beta}(u)$ is not identically zero, since C_a and C_β correspond to distinct points on Γ.

Choose a set of constants, $c_3, c_4, \cdots, c_m$ such that $\psi_i(c) \neq 0$, $\phi_{aa'}(c) \neq 0$ and $\theta_{a\beta}(c) \neq 0$ when $l_{2a} = l_{2\beta}$. Let

$$\xi = \sum_{j=3}^{m} c_i\xi_i.$$

We assert that *the curve* $L \equiv \{\xi_1, \xi_2, \xi\}$ *in* S_3 *is free from singularities both at finite distance and at infinity.* All points of L which do not correspond to points of the sets $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ are necessarily simple points. Moreover, if $\xi = d_i$ at A_i, then $\xi - d_i$ vanishes to the order one at A_i since $\psi_i(c) \neq 0$. The function ξ assumes distinct values at B_a and $B_{a'}$ since $\phi_{aa'}(c) \neq 0$. At any

pair of points C_α, C_β at which the values of ξ_2/ξ_1 are the same, the values of ξ/ξ_1 are distinct since $\theta_{\alpha\beta}(c) \neq 0$.

Finally, at any point C_a the quotients $1/\xi_1, \xi_2/\xi_1, \xi/\xi_1$ are finite and $1/\xi_1$ vanishes to the order one. Thus the points of L which correspond to the points in $\mathfrak{A}$, $\mathfrak{B}$ and $\mathfrak{C}$ are also simple points. This establishes Theorem 2.

4. Let the curve $C \equiv \{\lambda_0, \lambda_1, \cdots, \lambda_r\}$ be free from singularities in the projective space $S_r: (x_0, x_1, \cdots, x_r)$. By placing $x'_{ij} = x_i x_j$, $i, j = 0, 1, 2, \cdots, r$, we refer the hyperquadrics of S_r to the hyperplanes of a new space S_N in which the (x'_{ij}) are homogeneous coördinates. On placing $\lambda'_{ij} = \lambda_i\lambda_j$ we have defined in S_N a curve $C' \equiv \{\lambda'_{ij}\}$. Between C and C' there is a $1:1$ birational correspondence. A straightforward application of our definition of a simple point shows that C' is also free from singularities.

If P'_i, $i = 1, 2, 3$, are any three points of C' and P_1, P_2, P_3 the corresponding points of C, it is possible to find a hyperquadric in S_r passing through P_1 and P_2 but not through P_3, so that the corresponding hyperplane in S_N passes through P'_1 and P'_2 but not through P'_3. Thus no three points of C' are collinear. Similarly, any tangent line of C' has only its point of contact in common with C'.

We repeat this process, applying it on the hyperquadrics of S_N and the curve C'. We obtain thereby a curve C'' in $1:1$ birational correspondence with C' and hence also with C. Since no three points of C' are collinear, there exists a hyperquadric through any three given points of C' which does not pass through a given fourth point. Hence *no four points of C'' are coplanar.* In the same way we conclude from the above-mentioned property of the tangents to C' that *through any two points of C'' there passes a hyperplane which is tangent to C'' at one of them but not at the other.*

Let $\xi_1, \xi_2, \cdots, \xi_M$ be a set of elements in Σ which define the curve C''. (We have $M = \frac{1}{2}(N+2)(N+1) - 1$, the dimension of the space of hyperquadrics over S_N. Likewise, $N = \frac{1}{2}(r+2)(r+1) - 1$.) We assume that the elements $\xi_1, \cdots, \xi_M$ satisfy the conditions (1), (2) and (3) of Paragraph 2.

Let $u_1, u_2, \cdots, u_M$ be indeterminates and let $y = \sum_{i=1}^{M} u_i\xi_i$. The function y is connected with ξ_1 by an irreducible equation

$$f(\xi_1, y; u) = 0$$

of degree ν, where ν is the degree of Σ over $K(\xi_1)$. If $D(\xi_1, u)$ is the discriminant of f, then

$$D(\xi_1, u) = P^2(\xi_1, u)\Delta(\xi_1),$$

where P is a polynomial in ξ_1 and u, and Δ is the field discriminant of Σ, so that Δ is independent of u. Assume for the moment that the u's have special

values u^0 and let $y^0 = \Sigma u_i^0 \xi_i$, $P^0(\xi_i) = P(\xi_1, u^0)$. Let $\xi_1 = c$ be a root of $P^0(\xi_1)$. By known properties of the discriminant of f,[5] it follows that (1) either there must exist at least two distinct points of the Riemann surface of Σ at which $\xi_1 = c$ and at which also the values of y^0 are equal to each other; or (2) $y^0 = d$ at one of the points, say at P, at which $\xi_1 = c$, and $y^0 - d$ vanishes at P to an order larger than one. Since C'' is free from singularities, it is true that given any constant c, a linear combination of the ξ_i's can be found such that neither (1) nor (2) take place. For the corresponding values u^0 of the u_i, c will not be a root of $P(\xi_1, u_0)$. It follows that $P(\xi_1, u)$ as a polynomial in ξ_1, does not have roots independent of the u's.

For general values of the u_i, P has no multiple roots in ξ_1. Assuming the contrary, let $P(\xi_1, u)$ have the factor $Q(\xi_1, u)$ all of whose roots are multiple. Then if a is any constant, a sufficient condition that a be a multiple root of P is that the u's satisfy the equation $Q(a, u) = 0$. Hence our assertion will follow if we prove that two independent conditions (in fact linear conditions) are imposed on the indeterminates u by requiring that $\xi_1 = a$ be a multiple root of P.

If $(\xi_1 - a) = \mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdots \mathfrak{P}_\nu$ is the prime decomposition of the ideal $(\xi_1 - a)$ in the ring of integral functions of ξ_1 in Σ, (we may assume $\Delta(a) \neq 0$ so that each factor occurs only to the first power), then one of the following three conditions is necessary in order that $\xi_1 = a$ be a multiple root of P:

a) For some three of the ideals $\mathfrak{P}_i$, say $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{P}_3$, there exists a constant b such that

$$y - b \equiv 0 \ (\mathfrak{P}_1 \cdot \mathfrak{P}_2 \cdot \mathfrak{P}_3).$$

b) $y - b' \equiv 0 \ (\mathfrak{P}_1 \cdot \mathfrak{P}_2)$, $y - b'' \equiv 0 \ (\mathfrak{P}_3 \mathfrak{P}_4)$ for some constants b' and b'' and some four of the ideals $\mathfrak{P}_i$.

c) $y - b - c(\xi_1 - a) \equiv 0 \ (\mathfrak{P}_1^2 \cdot \mathfrak{P}_2^2)$ for some constants, b and c and some two of the ideals $\mathfrak{P}_i$.

If $\xi_i \equiv a_{ij} \ (\mathfrak{P}_j)$ then the matrix

$$A_1 = \begin{pmatrix} a_{11} - a_{12}, a_{21} - a_{22}, \cdots, a_{M1} - a_{M2} \\ a_{11} - a_{13}, a_{21} - a_{23}, \cdots, a_{M1} - a_{M3} \end{pmatrix}$$

is of rank two since otherwise the three points $(a_{1i}, a_{2i}, \cdots, a_{Mi})$, $i = 1, 2, 3$, on C'' would be collinear. Similarly, the matrix

$$A_2 = \begin{pmatrix} a_{11} - a_{12}, a_{21} - a_{22}, \cdots, a_{M1} - a_{M2} \\ a_{13} - a_{14}, a_{23} - a_{24}, \cdots, a_{M3} - a_{M4} \end{pmatrix}$$

[5] See e. g. Dedekind-Weber, "Theorie der algebraischen Funktionen einer Veränderlichen," *loc. cit.*

is of rank two since the four points $(a_{1i}, a_{2i}, \cdots, a_{Mi})$, $i = 1, 2, 3, 4$ cannot be coplanar.[6]

Since $\Delta(a) \neq 0$, $(\xi_1 - a)$ is a uniformizing parameter on each of the ideals $\mathfrak{P}_j$. Let $\dfrac{\xi_i - a_{ij}}{\xi_1 - a} = b_{ij}$ at $\mathfrak{P}_j$. The matrix

$$A_3 = \begin{pmatrix} a_{11} - a_{12}, \cdots, a_{M1} - a_{M2} \\ b_{11} - b_{12}, \cdots, b_{M1} - b_{M2} \end{pmatrix}$$

is of rank two. In the contrary case, any hyperplane through the points P_i: $(a_{1i}, a_{2i}, \cdots, a_{Mi})$, $i = 1, 2$ and tangent to C'' at P_1 would also be tangent to C'' at P_2.

In order that condition (a) be fulfilled, the quantities u must satisfy the equations

$$\sum_{j=1}^{M} (a_{j1} - a_{ji}) u_j = 0 \qquad (i = 2, 3).$$

Condition (b) requires that the equations

$$\sum_{j=1}^{M} (a_{j1} - a_{j2}) u_j = 0, \qquad \sum_{j=1}^{M} (a_{j3} - a_{j4}) u_j = 0$$

be satisfied. Finally, the equations

$$\sum_{j=1}^{M} (a_{j1} - a_{j2}) u_j = 0, \qquad \sum_{j=1}^{M} (b_{j1} - b_{j2}) u_j = 0$$

must be satisfied in order that (c) occur. Thus a, b, and c each impose two independent conditions on the indeterminates u. Hence $P(\xi_1, u)$ has no multiple roots for general values of u.

If $P_1, P_2, \cdots, P_\nu$ are the points of the Riemann surface where ξ_1 becomes infinite, and if $\xi_i/\xi_1 = \lambda_{ij}$ at P_j, then (as in Theorem 2),

$$\theta_{\alpha\beta}(u) = \sum_{i=1}^{M} (l_{i\alpha} - l_{i\beta}) u_i$$

is not identically zero if $\alpha \neq \beta$. Thus there exists a set of constants $c_1, c_2, \cdots, c_M$ such that $P(\xi_1, c)$ has only simple roots, none of which coincides with a root of $\Delta(\xi_1)$ and such that $\theta_{\alpha\beta}(c) \neq 0$. If

$$y = c_1\xi_1 + c_2\xi_2 + \cdots + c_M\xi_M,$$

then the curve $\{\xi_1, y\}$ has no singularities at infinity (since $\theta_{\alpha\beta}(c) \neq 0$) and has ordinary double points at finite distance corresponding to the roots of $P(\xi_1, c) = 0$. This proves Theorem 3.

THE JOHNS HOPKINS UNIVERSITY.

---

[6] Actually the condition imposed by us that no four points be coplanar is stronger than the one we actually use now concerning the ranks of the matrices A_1 and A_2. Since we are projecting our curve in S_M from a particular S_{M-2} at infinity we need only require that if four points on our curve are coplanar then lines joining pairs of them do not meet on this S_{M-2}.

PROPERTIES OF THE CUBIC SURFACE DERIVED FROM A NEW NORMAL FORM.*

By Arnold Emch.

1. Introduction. In a paper which appeared in the *American Journal of Mathematics,* vol. 53 (1931), pp. 902-910, I discussed a new normal form of the cubic surface

$$(1)\quad x_1^3 + x_2^3 + x_3^3 + x_4^3 - 3(a_1x_2x_3x_4 + a_2x_1x_3x_4 + a_3x_1x_2x_4 + a_4x_1x_2x_3) = 0$$

and its relation to the configuration Δ_{18} of the flexes formed by the syzygetic pencils of cubics cut out by the surface on the coördinate-planes. It is shown that the general cubic surface can be represented in this form in a finite number of ways only. The question whether there is only one way or several ways in which this can be done is not answered in that paper. In what follows I shall prove that there is more than one solution to this problem and incidentally prove some properties of the cubic surface which hitherto have been derived by sythetic methods only.

2. Further properties of the Δ_{18} configuration. Let F denote the cubic (1) and i, j, k, l the indices 1, 2, 3, 4 in any order; $\partial F/\partial x_i = F_i$; then

$$(2)\qquad F_i = 3[x_i^2 - (jx_kx_l + kx_lx_j + lx_jx_k).$$

For $x_4 = 0$, we have the syzygetic pencil of plane cubics

$$(3)\qquad x_1^3 + x_2^3 + x_3^3 - 3a_4x_1x_2x_3 = 0.$$

The flexes on the join $A_1A_2(x_3 = 0, x_4 = 0)$ are

$$(1, -1, 0, 0);\quad (1, -\omega, 0, 0);\quad (1, -\omega^2, 0, 0)$$

and the tangent planes to F at these points are

$$(3)\qquad \begin{aligned} x_1 + x_2 + a_4x_3 + a_3x_4 &= 0, \\ x_1 + \omega^2 x_2 + a_4\omega x_3 + a_3\omega x_4 &= 0, \\ x_1 + \omega x_2 + a_4\omega^2 x_3 + a_3\omega^2 x_4 &= 0. \end{aligned}$$

These intersect in the point $P(0, 0, a_3, -a_4)$, which lies on the join $A_3A_4(x_1 = 0, x_2 = 0)$ and also on the Hessian of F

* Received April 18, 1938.

$$(4)\quad H=\begin{vmatrix} -2x_1, & a_3x_4+a_4x_3, & a_4x_2+a_2x_4, & a_2x_3+a_3x_2 \\ a_3x_4+a_4x_3, & -2x_2, & a_1x_4+a_4x_1, & a_1x_3+a_3x_1 \\ a_4x_2+a_2x_4, & a_1x_4+a_4x_1, & -2x_3, & a_2x_1+a_1x_2 \\ a_2x_3+a_3x_2, & a_1x_3+a_3x_1, & a_2x_1+a_1x_2, & -2x_4 \end{vmatrix}.$$

Hence the polar quadric of P must be a cone, which in fact becomes

$$(5)\qquad a_3x_3^2-a_4x_4^2-(a_3x_4-a_4x_3)(a_1x_2+a_2x_1)=0.$$

The vertex of this cone is at $Q(a_1,-a_2,0,0)$ which lies on the join $A_1A_2(x_3=0,x_4=0)$. In a similar manner it is found that the triples of tangent planes to F at the remaining flexes of Δ_{18} on the joins A_2A_3, A_1A_4; A_3A_1, A_2A_4 meet in the points

$$R(a_1,0,0,-a_4),\quad S(0,a_2,-a_3,0),\quad T(0,a_2,0,-a_4),\quad U(a_1,0,-a_3,0)$$

respectively. R and S as well as T and U are also conjugate points on H. The three couples (P,Q); (R,S); (T,U) lie on the plane

$$(6)\qquad \alpha=a_2a_3a_4x_1+a_1a_3a_4x_2+a_1a_2a_4x_3+a_1a_2a_3x_4=0$$

and are obviously the six vertices of the quadrilateral cut out on (6) by the coördinate-planes. The polar plane (2 polar) of a generic point (y) with respect to F is

$$(7)\qquad \Sigma[y_i^2-(a_jy_ky_l+a_kx_lx_j+a_lx_jx_k]=0.$$

The diagonal points of the quadrilateral on α are $D_1(a_1,-a_2,-a_3,a_4)$;

$$D_2(a_1,-a_2,a_3,-a_4);\quad D_3(a_1,a_2,-a_3,-a_4).$$

By (7) it is verified immediately that D_1, D_2, D_3 all have the same polar-plane

$$(8)\qquad \beta=\Sigma(a_i^2+a_ja_ka_l)x_i=0.$$

The polar plane of A_i is obviously $x_i=0$, $i=1,2,3,4$. The D's are not on F nor on H. These results may be summed up in

THEOREM 1. *The tangent-planes to the cubic surface at the flexes of the four syzygetic pencils of plane cubics meet by threes, corresponding to each edge of $A_1A_2A_3A_4$, in six points of the plane α, which are the vertices of the quadrilateral cut out on α by the four faces of the coördinate tetrahedron. The six points are on the Hessian of the cubic surface and form three couples of conjugate points, one on each pair of opposite edges of the tetrahedron. The diagonal points of the quadrilateral have the same polar plane.*

3. Character of plane sections of Hessian. Polar quartics of lines. Polar class cubics of planes.

1. The line

$$QS = (a_1, -a_2, 0, 0) \times (0, a_2, -a_3, 0),$$

or

$$\{\lambda a_1, a_2(1-\lambda), -a_3, 0\}$$

cuts H in a point W_4, outside of Q, S, U, whose cöordinates are obtained as

$$W_4\{a_1^2(a_2^3-a_3^3)(a_1^2-a_2a_3a_4),\\ a_2^2(a_3^3-a_1^3)(a_2^2-a_1a_3a_4),\ a_3^2(a_1^3-a_2^3)(a_3^2-a_1a_2a_4), 0\}.$$

Similarly the remaining three lines of the quadrilateral intersect H in

$$W_3\{a_1^2(a_2^3-a_4^3)(a_1^2-a_2a_3a_4),\\ a_2^2(a_4^3-a_1^3)(a_2^2-a_1a_3a_4), 0,\ a_4^2(a_1^3-a_3^3)(a_4^2-a_1a_2a_3)\},$$

$$W_2\{a_1^2(a_3^3-a_4^3)(a_1^2-a_2a_3a_4),\\ 0, a_3^2(a_4^3-a_1^3)(a_3^2-a_1a_2a_4),\ a_4^2(a_1^3-a_3^3)(a_4^2-a_1a_2a_3)\},$$

$$W_1\{0, a_2^2(a_3^3-a_4^3)(a_2^2-a_1a_3a_4),\\ a_3^2(a_4^3-a_2^3)(a_3^2-a_1a_2a_4),\ a_4^2(a_2^3-a_3^3)(a_4^2-a_1a_2a_3)\}.$$

By using the parametric representation of, say W_4W_3 it is not difficult to show that W_1 and W_2 lie on the join of W_3 and W_4, i. e., the four W's are collinear on a line w. Denoting the lines of the quadrilateral on α by q_1, q_2, q_3, q_4 we thus see that *these lines together with w form a pentalateral whose 10 points of intersection P, Q, R, S, T, U, W_1, W_2, W_3, W_4 lie on the Hessian. From this follows that the intersection $H\alpha$ of H with α is a Lüroth-quartic.*

This follows, of course, also from the more general result that a generic plane section of H is such a curve.

2. The polar plane of a point (λ) on the join d_3 of $P(0, 0, a_3, -a_4)$ and $Q(a_1, -a_2, 0, 0)$, i. e., $(\lambda a_1, -\lambda a_2, a_3, -a_4)$, according to (7), is

$$(9)\qquad (a_1^2x_1 + a_2^2x_2 + a_1a_2a_4x_3 + a_1a_2a_3x_4)\lambda^2 \\ + (a_2a_3a_4x_1 + a_1a_3a_4x_2 + a_1a_2a_4x_3 + a_1a_2a_4x_1) = 0$$

and passes through the diagonal points D_1 and D_2. From (9) is seen that the polar planes of the points of d_3 all pass through the line of intersection d'_3 of the planes represented by the parentheses of (9). Moreover it is clear that d'_3 lies on the plane $\beta = \Sigma(a_1^2 + a_2a_3a_4)x_1 + \cdots$. The polar quadrics of the points of d'_3 all pass through d_3 and form a pencil on a base-quartic.

But since the latter contains d_3, this quartic has a residual cubic. The four quadric cones of the pencil coincide by twos, so that the vertices P_1 and P_2 of these double cones lie on d_3 and also on H. The conjugates P'_1 and P'_2 of P_1 and P_2 lie on d'_3 and must be counted doubly on this line. Thus d'_3 is a double tangent of the Hessian. The same is true of d'_1 and d'_2, similarly attached to d_1 and d_2, the joins of R, S, and T, U. Hence the known

THEOREM 2. *The axes d'_1, d'_2, d'_3 of the pencils of polar planes corresponding to the points of the diagonals d_1, d_2, d_3 of the quadrilateral $q_1q_2q_3q_4$ in the plane α are double tangents of the Hessian.*

3. The polar planes of $q_1 = QU(a_1\lambda, d_2(1-\lambda), -a_3, 0)$ envelope the conic

$$\begin{aligned}(a_1^2x_1 + a_2^2x_2 + a_1a_2a_4x_3 + a_1a_2a_3x_4)\lambda^2 \\ - [a_2a_3a_4x_1 + (2a_2^2 - a_1a_3a_4)x_2 + a_1a_2a_4x_3 + a_1a_2a_3x_4]\lambda \\ + a_2a_3a_4x_1 + a_2^2x_2 + a_3^2x_3 + a_1a_2a_3x_4 = 0.\end{aligned}$$

If we write this $A\lambda^2 + B\lambda + C = 0$, the vertex V_4 of this cone is obtained as the intersection of $A = B = C = 0$,

$$(10) \quad V_4 \begin{cases} \rho x_1 = a_1a_2a_3(a_2^2 - a_1a_3a_4)(a_3^2 - a_1a_2a_4) \\ \rho x_2 = a_1a_2a_3(a_3^2 - a_1a_2a_4)(a_1^2 - a_2a_3a_4) \\ \rho x_3 = a_1a_2a_3(a_1^2 - a_2a_3a_4)(a_2^2 - a_1a_3a_4) \\ \rho x_4 = a_4(a_1^3a_2^3 + a_2^3a_3^3 + a_3^3a_1^3 - a_1^2a_2^2a_3^2a_4^2) - 2a_1^2a_2^2a_3^2. \end{cases}$$

This is the conjugate of W_4 on the Hessian. In a similar manner the points V_3, V_2, V_1 as the conjugates of W_3, W_2, W_1 are obtained. From the analytic expressions of the V's, as in (10), it is easily verified that the six edges of the tetrahedron $V_1V_2V_3V_4$ pass through the 6 vertices of the quadrilateral $q_1q_2q_3q_4$. For the sake of brevity this arduous computation is omitted.

Now the polar planes of the points of α envelope a surface S_α of class 4 and order 3, as is well known. It is a Cayley cubic with V_1, V_2, V_3, V_4 as nodes, which touches the Hessian along a sextic C_6 which is the conjugate of the plane sextic H_α. If M and N are conjugate points on H, then the polar planes of M and N touch H at N and M respectively. From this follows that C_6 passes through the 6 vertices $P, Q, \cdots$ of $q_1q_2q_3q_4$. It is of genus 3 and a so-called Wirtinger sextic. Its trisecants form a ruled octic surface R_8. To prove that H_α is a residual intersection of R_8 with α, let t be any trisecant cutting C_6 in R_1, R_2, R_3. The polar cones of these determine a pencil of quadrics on the 8 associated points of the net of polar quadrics of points of α.

Among these is a fourth conic whose vertex V is on C_6 and whose conjugate V' lies on α and also on t. Hence t cuts α in a point of H_α. We may therefore state

THEOREM 3. *The polar cubic surface of the plane α touches F along a Wirtinger sextic C_6. The ruled octic surface of trisecants of C_6 cuts α in $q_1q_2q_3q_4$ and the residual H_α. The C_6 passes through the 10 nodes of the Hessian. The polar cones of $V_1V_2V_3V_4$ touch α along $q_1q_2q_3q_4$. The joins V_iV_k touch H at their initersection with α.*

The last three parts of this theorem are known but are added for the sake of completeness.

4. The summit plane α.

1. Looking at the form of (1) and the couples of conjugate points, like $P(0, 0, a_3, -a_4)$; $Q(a_1, -a_2, 0, 0)$ etc. in the plane α, it is clear that by multiplying the second part of (1) by a parameter c, the points $P, Q, \cdots$ remain the same. Hence the *quadrilateral $q_1q_2q_3q_4$ is common to a whole pencil of cubics, and in the same capacity, α is common to every cubic of the pencil.*

P and Q may always be chosen in such a way that they form the vertices of two conjugate Steineran trihedrals. There are 120 such couples. Each gives rise to representation of the cubic in the form

$$UVW - cU'V'W' = 0, \tag{11}$$

which reveals at once 9 of the 27 lines of the cubic, such that each of the planes $U\cdots, U'\cdots$ is a tritangent plane containing 3 of the 9 lines.

I shall now investigate the possibility of representing (1) in the form (11), with $P = (U' = V' = W' = 0)$, $Q = (U = V = W = 0)$. Such a cubic may be written in the form

$$\begin{aligned} F^* = {} & (a_2x_1 + a_1x_2 + \lambda_1x_3 + \mu_1x_4)(a_2x_1 + a_1x_2 + \lambda_2x_3 + \mu_2x_4) \\ & \times (a_2x_1 + a_1x_2 + \lambda_3x_3 + \mu_3x_4) - c(\delta_1x_1 + \tau_1x_2 + a_4x_3 + a_3x_4) \\ & \times (\delta_2x_1 + \tau_2x_2 + a_4x_3 + a_3x_4)(\delta_3x_1 + \tau_3x_2 + a_4x_3 + a_3x_4) = 0, \end{aligned} \tag{12}$$

which clearly has P and Q as vertices of a couple of conjugate trihedrals on the Hessian of (1). Expanding and denoting the coefficients of $x_ix_kx_l$ by a_{ikl}, we have first the condition that all terms containing a square of a variable, like $x_i^2x_k$ vanish. Thus

$$
(13)\quad
\begin{array}{rl}
1. & a_{112} = 3a_1a_2^2 - c(\delta_1\delta_2\tau_3 + \delta_2\delta_3\tau_1 + \delta_3\delta_1\tau_2) = 0 \\
2. & a_{113} = a_2^2(\lambda_1 + \lambda_2 + \lambda_3) - ca_4(\delta_1\delta_2 + \delta_2\delta_3 + \delta_3\delta_1) = 0 \\
3. & a_{114} = a_2^2(\mu_1 + \mu_2 + \mu_3) - ca_3(\delta_1\delta_2 + \delta_2\delta_3 + \delta_3\delta_1) = 0 \\
4. & a_{112} = 3a_1^2a_2 - c(\tau_1\tau_2\delta_3 + \tau_2\tau_3\delta_1 + \tau_3\tau_1\delta_2) = 0 \\
5. & a_{223} = a_1^2(\lambda_1 + \lambda_2 + \lambda_3) - ca_4(\tau_1\tau_2 + \tau_2\tau_3 + \tau_3\tau_1) = 0 \\
6. & a_{224} = a_1^2(\mu_1 + \mu_2 + \mu_3) - ca_3(\tau_1\tau_2 + \tau_2\tau_3 + \tau_3\tau_1) = 0 \\
7. & a_{133} = a_2(\lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1) - ca_4^2(\delta_1 + \delta_2 + \delta_3) = 0 \\
8. & a_{233} = a_1(\lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1) - ca_4^2(\tau_1 + \tau_2 + \tau_3) = 0 \\
9. & a_{334} = \mu_1\lambda_2\lambda_3 + \mu_2\lambda_3\lambda_1 + \mu_1\lambda_1\lambda_2 - 3ca_3a_4^2 = 0 \\
10. & a_{114} = a_2(\mu_1\mu_2 + \mu_2\mu_3 + \mu_3\mu_1) - ca_3^2(\delta_1 + \delta_2 + \delta_3) = 0 \\
11. & a_{224} = a_1(\mu_1\mu_2 + \mu_2\mu_3 + \mu_3\mu_1) - ca_3^2(\tau_1 + \tau_2 + \tau_3) = 0 \\
12. & a_{334} = \lambda_3\mu_1\mu_2 + \lambda_1\mu_2\mu_3 + \lambda_2\mu_3\mu_1 - 3ca_3^2a_4 = 0.
\end{array}
$$

The λ, μ, δ, τ must be determined such that these 12 equations are satisfied. First we show that this system can be reduced to eight equations. From 2, and 3., as well as 5. and 6., follows

$$(13)\qquad a_3(\lambda_1 + \lambda_2 + \lambda_3) - a_4(\mu_1 + \mu_2 + \mu_3) = 0.$$

Likewise from 7. and 8., and 10. and 11.,

$$(14)\qquad a_1(\delta_1 + \delta_2 + \delta_3) - a_2(\tau_1 + \tau_2 + \tau_3) = 0.$$

Hence 2. and 3. may be replaced by 2. and 13., 5. and 6. by 5. and 13., which reduces 2., 3., 5., 6. to 2., 5., 13. Similarly, 7., 8., 10., 11., may be reduced to 7., 10., 14. Moreover 7., 9., 10., 12. may be replaced by

$$(15)\qquad \frac{(\lambda_1\mu_2\mu_3 + \lambda_2\mu_3\mu_1 + \lambda_3\mu_1\mu_2)^2}{(\lambda_1\lambda_2\mu_3 + \lambda_2\lambda_3\mu_1 + \lambda_3\lambda_1\mu_2)^2} = \frac{\dfrac{a_2(\mu_1\mu_2 + \mu_2\mu_3 + \mu_3\mu_1)}{c(\delta_1 + \delta_2 + \delta_3)}}{\dfrac{a_2(\lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1)}{c(\delta_1 + \delta_2 + \delta_3)}},$$

$$\lambda_1\mu_2\mu_3 + \lambda_2\mu_3\mu_1 + \lambda_3\mu_1\mu_2 = 3ca_3^2a_4, \quad \lambda_1\lambda_2\mu_3 + \lambda_2\lambda_3\mu_1 + \lambda_3\lambda_1\mu_2 = 3ca_3a_4^2,$$

i. e., 12. and 9. In a similar manner 1., 2., 4., 5., may be reduced to three. Hence the entire system (13) may be replaced by 8 equations.

Next write down the coefficients a_{jkl} of $a_ix_jx_kx_l$, $i \neq j \neq k \neq l$,

$$
(16)\quad
\begin{aligned}
a_{123} &= a_1a_2\frac{\lambda_1 + \lambda_2 + \lambda_3}{a_4} - c[\delta_1(\tau_2 + \tau_3) + \delta_2(\tau_3 + \tau_1) + \delta_3(\tau_1 + \tau_2)], \\
a_{124} &= a_1a_2\frac{\mu_1 + \mu_2 + \mu_3}{a_3} - c[\delta_1(\tau_2 + \tau_3) + \delta_2(\tau_3 + \tau_1) + \delta_3(\tau_1 + \tau_2)], \\
a_{134} &= \lambda_1(\mu_2 + \mu_3) + \lambda_2(\mu_3 + \mu_1) + \lambda_3(\mu_1 + \mu_2) - ca_3a_4\frac{\delta_1 + \delta_2 + \delta_3}{a_2}, \\
a_{234} &= \lambda_1(\mu_2 + \mu_3) + \lambda_2(\mu_3 + \mu_1) + \lambda_3(\mu_1 + \mu_2) - ca_3a_4\frac{\tau_1 + \tau_2 + \tau_3}{a_1}.
\end{aligned}
$$

On account of 13. and 14., $a_{123}=a_{124}$; $a_{134}=a_{234}$. Hence $a_{123}=a_{124}=a_{134}=a_{234}$, when $a_{124}=a_{134}$. This adds one to eight conditions. Lastly, we have the three conditions for the coefficients of x_i^3

$$(17)\qquad a_2^3-c\delta_1\delta_2\delta_3=a_1^3-c\tau_1\tau_2\tau_3=\lambda_1\lambda_2\lambda_3-ca_4^3=\mu_1\mu_2\mu_3-ca_3^3.$$

The entire system thus is reduced to 12 equations with the 12 unknowns $\lambda_i, \mu_i, \delta_i, \tau_i$, $i=1,2,3$. Solving for these and then dividing the entire equation (12) by the common value of (17), the parameter c can then be chosen such that in the reduced equation of (12) to the form (1) the parameter of the parenthesis of $\Sigma a_i x_j x_k x_l$ becomes -3. The form (12) can therefore be reduced to the form (1). The same process may be repeated on the couples of conjugate points of H; R, S and T, U. From this follows that the normal form (1) may be represented in three different ways by Salmon's normal form (11), and that these represent three couples of associated Steinerian trihedrals, whose vertices (P, Q); (R, S); (T, U) lie in the plane α defined by A. L. Dixon [1] and others as a *summit-plane.* The three couples contain all the 27 lines of the cubic. This fact was already discovered by Steiner,[2] who failed to realize that the three couples of vertices are coplanar.

2. Steiner, in the paper referred to, stated that there are 120 couples of conjugate trihedrals, and that these arrange themselves in 40 triples of conjugate pairs, each of which contains all 27 lines. From Dixon's (and others) investigations follows that with every general cubic surface are associated 40 sumit-planes with the Steiner property.

It now remains to show the connection between these summit-planes and the possibilities of representing the cubic in the normal form

$$(14)\qquad \begin{aligned}&\alpha_1^3+\alpha_2^3+\alpha_3^3+\alpha_4^3\\ &\qquad -3(b_1\alpha_2\alpha_3\alpha_4+b_2\alpha_1\alpha_3\alpha_4+b_3\alpha_1\alpha_2\alpha_4+b_4\alpha_1\alpha_2\alpha_3)=0.\end{aligned}$$

In the first place we can form ∞^{15} pentalaterals in projective space S_3, like $x_1=x_2=x_3=x_4=\alpha=0$, or $\alpha, \alpha_1, \alpha_2, \alpha_3, \alpha_4$. Considering the plane α in the preceding discussion, we can choose ∞^8 quadrilaterals $q_1q_2q_3q_4$ in α. Through each of these we can pass ∞^4 tetralaterals $\alpha_1\alpha_2\alpha_3\alpha_4$. Then form the cubic (14). The coefficients b_1, b_2, b_3, b_4 can be chosen such that

$$(15)\qquad \Sigma\frac{\alpha_i}{b_i}=\Sigma\frac{x_i}{\alpha_i}=\alpha.$$

[1] *Proceedings of the London Mathematical Society,* 2nd ser., vol. 37 (1934).

[2] Journal für reine und angewandte Mathematik, vol. 53 (1856), pp. 133-141; *Werke,* vol. 2, pp. 652-659.

$\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0$ pass respectively through q_1, q_2, q_3, q_4. Hence through every quadrilateral in a plane α there are ∞^4 tetrahedrals $\alpha_1\alpha_2\alpha_3\alpha_4$ which together with α form the basis for a normal representation (1). Hence all of the ∞^{19} general cubics may be put in the form (1) as was proved before.

The representation of the cubic in the form (11) with P and Q as given vertices of a couple of conjugate Steinerian trihedrals is unique. Assuming another representation of the same cubic with the same vertices P and Q, say $U_1V_1W_1 - c_1U'_1V'_1W'_1$, the intersection of $U = 0$ and $U'_1 = 0$ would have six points in common with the surface which is not possible. The same is true of any other couple like $W = 0$ and $V'_1 = 0$. From this follows that the representation of (1) in the form (12) is unique, although the solution of the system of equations (13), etc. would indicate a finite number of solutions greater than 1. The algebraic proof for a unique compatible solution from those equations seems to be an arduous task and shall not be attempted here.

3. Now let $\alpha^{(i)}$, $i = 2, 3, \cdots, 40$ be any of the other 39 summit-planes outside of α, and $q_1q_2q_3q_4$ again the quadrilateral containing the triple of associated couples of conjugate vertices. There are ∞^4 cubics of the form (14) on this quadrilateral. Among these is the given cubic. From this follows

THEOREM 4. *The general cubic surface may be represented in* 40 *different ways in the normal form*

$$\alpha_1^3 + \alpha_2^3 + \alpha_3^3 + \alpha_4^3 - 3(b_1\alpha_2\alpha_3\alpha_4 + b_2\alpha_1\alpha_3\alpha_4 + b_3\alpha_1\alpha_2\alpha_4 + b_4\alpha_1\alpha_2\alpha_3) = 0,$$

one associated with each of the 40 *summit planes.*

UNIVERSITY OF ILLINOIS.

THE EQUATION OF MOTION OF EQUAL MAPS.* [1]

By J. R. Musselman.

1. If we wish to move an object from one position on a plane to another position on the same plane, we may apply the theory of rotation. This theory is well known, and its equation [2] of motion is

$$y = tx + b.$$

It is the purpose of this paper to discuss a type of motion which will send an object into three or more positions consecutively on the same plane. Or if we prefer, we may think of three or more equal objects lying on a plane and ask for the equation of motion which will pick up all of them. For convenience, we shall call these equal objects maps.

2. A map M_1 lies on some reference plane, both with their own reference frames. We shall let x_1 be the name in the reference plane of the overlying point y in the map M_1. Then x and y are connected by the relation

$$\alpha_1 x_1 = y_1 + a_1, \qquad |\alpha_1| = 1. \tag{2.1}$$

If a second map M_2, equal to M_1, lies on the reference plane, we shall let x_2 be the name in the reference plane of the overlying point y in the map M_2. Thus we have

$$\alpha_2 x_2 = y + a_2, \qquad |\alpha_2| = 1. \tag{2.2}$$

Now x_1 and x_2 are corresponding points in the reference plane. They coincide at the fixed point

$$x_{12} = \frac{a_1}{\alpha_1 - \alpha_2} + \frac{a_2}{\alpha_2 - \alpha_1}. \tag{2.3}$$

For three equal maps we would have three fixed points x_{23}, x_{31} and x_{12} lying on the circle C_{123}, whose equation is

* Received March 9, 1938.

[1] The writer is indebted for suggestions to the late Professor Morley, who discussed a mechanical device for generating the motion for the case $n = 4$ before the International Congress at Oslo.

[2] Circular coördinates are used, i. e. y, x, b are complex numbers, t is a turn, $|t| = 1$. See F. Morley, "On an equation of planar motion." *American Journal of Mathematics*, vol. 47 (1925), pp. 98-100.

$$x = \sum^{3} \frac{a_1(\alpha_1 - T)}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)}. \tag{2.4}$$

The center, c_0, of this circle is given by

$$c_0 = \sum^{3} \frac{a_1\alpha_1}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)},$$

and its radius is the absolute value of c_1, where

$$c_1 = \sum^{3} \frac{a_1}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)}.$$

If c_1 vanishes we have

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ 1 & 1 & 1 \end{vmatrix} = 0 \tag{2.5}$$

and hence $x_{23} = x_{31} = x_{12}$. For four equal maps the circles C_{123}, C_{234}, C_{341} and C_{412} are included in

$$x = \sum^{4} \frac{a_1(\alpha_1 - T)(\alpha_1 - t)}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)}. \tag{2.6}$$

From the form of this equation we see that the circles are all osculants [3] of the limaçon

$$x = \sum^{4} \frac{a_1(\alpha_1 - T)^2}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)} = c_0 - 2c_1T + c_2T^2$$

i. e., they touch the curve at the points with parameter α_i and are on the node. The four centers of the four circles lie on the circle

$$x = \sum^{4} \frac{a_1\alpha_1(\alpha_1 - T)}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)} \tag{2.8}$$

with its center

$$c'_0 = \sum^{4} \frac{a_1\alpha_1^2}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_1 - \alpha_4)}.$$

This argument can be repeated indefinitely. Hence we can state the theorem *that for n equal maps there is a covariant circle, which is independent of the reference plane, such that for $n-1$ out of the n maps the n circles meet at a point and the n centers of these circles lie on a circle.* We call this covariant circle the centric circle.

3. For three maps, when c_1 does not vanish, we have three fixed points

[3] For the theory of osculants, see F. Morley and F. V. Morley, *Inversive Geometry* (1933), p. 261. This book will be referred to later as M.

x_{23}, x_{31} and x_{12} lying on the circle C_{123} whose equation is given in (2.4). If we use this circle as the base circle, the fixed points are now named respectively α_1, α_2 and α_3 and

$$\frac{a_2 - a_3}{\alpha_2 - \alpha_3} = \alpha_1, \text{ etc.},$$

so that

$$a_1 = K - \alpha_2\alpha_3.$$

We choose our constant so that

$$(3.1) \qquad a_1 = \alpha_1(\alpha_2 + \alpha_3).$$

Substituting this value of a_1 in (2.1) we have

$$(3.2) \qquad \alpha_1 x_1 = y + \alpha_1(\alpha_2 + \alpha_3).$$

Similarly

$$\alpha_2 x_2 = y + \alpha_2(\alpha_3 + \alpha_1).$$

Hence two corresponding points x_1 and x_2 are related by

$$(3.3) \qquad \alpha_1 x_1 - \alpha_2 x_2 = (\alpha_1 - \alpha_2)\alpha_3$$

or

$$(3.4) \qquad \alpha_1(x_1 - \alpha_2 - \alpha_3) = \alpha_2(x_2 - \alpha_3 - \alpha_1) = -\alpha_1\alpha_2\alpha_3\bar{x} \text{ say.}$$

That is, corresponding points are given in terms of an arbitrary $\bar{x}$ by

$$(3.5) \qquad x_1 + \alpha_2\alpha_3\bar{x} = \alpha_2 + \alpha_3.$$

Thus the three maps can be considered as the reflexions [4] of a fourth map M in the joins of the fixed points α_1, α_2 and α_3. Three corresponding points x_1, x_2 and x_3 can lie on a line when x is on the circumcircle of $\alpha_1\alpha_2\alpha_3$. In this case the line is the line of images of the point x and is on the orthocenter [5] of $\alpha_1\alpha_2\alpha_3$, namely $s_1 = \alpha_1 + \alpha_2 + \alpha_3$. If corresponding lines meet at a point, they must be the reflexions in the sides of $\alpha_1\alpha_2\alpha_3$ of some line on s_1; i. e., the corresponding lines are on the points $-\alpha_2\alpha_3/\alpha_1$, $-\alpha_3\alpha_1/\alpha_2$, $-\alpha_1\alpha_2/\alpha_3$ respectively, and their point of concurrence is on the circumcircle of $\alpha_1\alpha_2\alpha_3$. To construct this point one need only note that its Simson line is parallel to the given line on s_1.

4. Let us now consider the equation (3.1) which when combined with

---

[4] F. Morley, "On reflexive geometry," *Transactions of the American Mathematical Society*, vol. 8 (1907), pp. 14-24, also M, p. 187.

[5] F. Morley, "Orthocentric properties of the plane n-line," *Transactions of the American Mathematical Society*, vol. 4 (1902), pp. 1-12; also *M*, p. 187.

(2.1) gives the relation between the point x, in the reference plane and the overlying point y in the map M_1. It is

$$\alpha_1 x_1 = y + \alpha_1(\alpha_2 + \alpha_3)$$

or

$$\alpha_1(x_1 - s_1 + \alpha_1) = y.$$

If we change the origin by writing x for $x_1 - s_1$, we have the equation of motion of the map over the reference plane to be of the form

$$y = Tx + T^2, \qquad |T| = 1. \tag{4.1}$$

This is the equation of the motion of a map which takes three positions, where x is the point in the reference plane and y is the name of the point in the moving map which overlies x. Also, $x = 0$ is the orthocenter of the three fixed points. If, for instance, y is Washington, then the trace of Washington in the reference plane is

$$w = Tx + T^2$$

or

$$x = w/T - T \tag{4.2}$$

which is an ellipse. Since

$$\bar{x} = \bar{w}T - 1/T$$

$$\bar{w}x + \bar{x} = (w\bar{w} - 1)/T. \tag{4.3}$$

Hence if $w\bar{w} - 1 = 0$, *i. e.*, if w is a point on the circumcircle of the fixed points then

$$\bar{w}x + \bar{x} = 0,$$

and the trace of x is no longer an ellipse, but a segment, and *the three positions of Washington in the reference plane are on a line, and this line is on the orthocenter $x = 0$, of the three fixed points.* The equation of motion (4.1) is a da Vinci motion (M, p. 181).

Since any three points are connected by the relation

$$T^3 - s_1 T^2 + s_2 T - s_3 = 0 \tag{4.4}$$

or

$$T^2 = s_1 T - s_2 + s_3/T \tag{4.5}$$

we have, upon substituting (4.5) in (4.1)

$$y = Tx + s_1 T - s_2 + s_3/T,$$

which by change of origin can be written in the form

$$(4.6) \qquad y = x/T - T.$$

In comparing (4. 6) with (4. 2) we see that the rôle of the points x and y are interchanged. Consequently we can state that if y moves over a line on the orthocenter in the moving map, x in the reference plane is on the circumcircle of the fixed points and thus *the three lines traced out in the reference plane are concurrent.*

The important idea for the reader is to observe that a da Vinci motion (4. 1) is the natural and proper motion for three positions of an object, just as a rotation applies to two positions of an object. A da Vinci motion, of course, applies in many ways also to two positions of an object.

5. For four maps we saw that the four circles C_{123}, C_{234}, C_{341} and C_{412} are osculants of the limaçon (2. 7). By suitable choice of the reference frame we can take the limaçon as

$$(5.1) \qquad x = 2\mu t - t^2, \qquad (\mu \text{ real}).$$

The node of the limaçon is at $x = 1$, the focus at $x = \mu^2$. The osculant circle at $t = \alpha_1$ is

$$(5.2) \qquad C_{234}: \quad x = \mu(t + \alpha_1) - t\alpha_1.$$

Two such circles C_{234} and C_{341} meet at

$$(5.3) \qquad x_{34} = \mu(\alpha_1 + \alpha_2) - \alpha_1\alpha_2.$$

The six points of intersection of these four circles are the fixed points. They are the images of the node in the joins of the four points $\mu\alpha_i$ which lie on the centric circle.

It is clear that four corresponding points can lie on a line—the line that joins the orthocenters of say $x_{23}x_{31}x_{12}$ and $x_{34}x_{42}x_{23}$. Thus the line is on all four orthocenters. Analytically the orthocenter of $x_{34}x_{42}x_{23}$ is

$$x = \mu(\alpha_1 + z) - \alpha_1 z \qquad (z = \alpha_2 + \alpha_3 + \alpha_4).$$

It is then

$$x = \mu\sigma_1 - \alpha_1(\alpha_2 + \alpha_3 + \alpha_4), \qquad \sigma_1 = \sum^4 \alpha_i.$$

Since

$$\sigma_4\bar{x} = \mu\sigma_3 - \alpha_2\alpha_3 - \alpha_3\alpha_4 - \alpha_4\alpha_2$$

the equation of the line is

$$(5.4) \qquad x + \sigma_4\bar{x} = \mu(\sigma_1 + \sigma_3) - \sigma_2.$$

It is also clear that four corresponding lines can meet in a point. The point must be on all the circumcircles, hence it is *the node of the limaçon.*

6. The relation between corresponding points x_1 and x_2 of the maps M_1 and M_2 is from (3.3) and (5.3)

$$\alpha_1 x_1 - \alpha_2 x_2 = (\alpha_1 - \alpha_2) x_{12} = (\alpha_1 - \alpha_2)[\mu(\alpha_3 + \alpha_4) - \alpha_3\alpha_4]$$

or

$$\alpha_1\{x_1 - \mu(\alpha_2 + \alpha_3 + \alpha_4) + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_2\}$$
$$= \alpha_2\{x_2 - \mu(\alpha_3 + \alpha_4 + \alpha_1) + \alpha_3\alpha_4 + \alpha_4\alpha_1 + \alpha_1\alpha_3\} = \sigma_4\bar{x} \text{ say.}$$

That is, corresponding points are given in terms of an arbitrary $\bar{x}$ by

$$(6.1) \qquad \alpha_1\{x - \mu(\alpha_2 + \alpha_3 + \alpha_4) + \alpha_2\alpha_3 + \alpha_3\alpha_4 + \alpha_4\alpha_2\} - \sigma_4\bar{x} = 0.$$

This is a reflexion when $\mu = 1$; i.e., when the limaçon becomes a cardioid. In this case the maps are the reflexions of a map in four lines. The fixed points are the joins of the four lines. In general when n maps are the reflexions of a map in n lines, the theory becomes the theory of the n lines, and the Clifford chain [6] then enters.

Another special case is when $\mu = 0$. The fixed points are then $x_{12} = -\alpha_3\alpha_4$; i.e., they lie on a circle, and the three chords $x_{12} - x_{34}$, $x_{13} - x_{24}$, $x_{14} - x_{23}$ are parallel. Corresponding points are now given by

$$\alpha_1 x_1 + \sigma_3 - \alpha_2\alpha_3\alpha_4 - \sigma_4\bar{x} = 0$$

or

$$x_1 = (\bar{x}\sigma_4 - \sigma_3)/\alpha_1 + \sigma_4/\alpha_1^2.$$

Hence they lie on a limaçon

$$x = z/t + \sigma_4/t^2.$$

All such limaçons have the same center, and their nodes lie on the base circle.

7. To determine the equation of motion which picks up the four maps we write (6.1) as

$$\alpha_1 x_1 - \mu(\sigma_2 - \alpha_1\sigma_1 + \alpha_1^2) + \sigma_3 - \sigma_4/\alpha_1 = \sigma_4 y$$

or setting $x_1 = x$, $\alpha_1 = t$, we have the equation of motion in the form

$$(7.1) \qquad \sigma_4 y = tx - \mu(\sigma_2 - t\sigma_1 + t^2) + \sigma_3 - \sigma_4/t.$$

Since any four points are connected by

---

[6] F. Morley, "Extensions of Clifford's chain-theorem," *American Journal of Mathematics*, vol. 51 (1929), pp. 465-472; also M, p. 268.

$$t^4 - \sigma_1 t^3 + \sigma_2 t^2 - \sigma_3 t + \sigma_4 = 0$$

we have

$$\sigma_3 - \sigma_4/t = t^3 - \sigma_1 t^2 + \sigma_2 t.$$

Hence (7.1) can be written

$$\sigma_4 y = -\mu\sigma_2 + t(x + \mu\sigma_1 + \sigma_2) - t^2(\mu + \sigma_1) + t^3$$

which, with a change of origin, is of the form

$$y + b = tx + at^2 + t^3$$

or

$$x = (y + b)/t - at - t^2. \tag{7.2}$$

Since (7.2) for x is precisely of the form (7.1) for y, we see that, as in the case for three maps, the rôles of the point x in the reference plane and of the point y, which overlies it, in the moving plane, are interchangeable.

We have shown that the natural and proper equations of motion for two, three, and four equal maps are of the form

$$\begin{aligned} y &= tx \\ y &= tx + t^2 \\ y &= tx + at^2 + t^3. \end{aligned}$$

The theory as developed above can be extended to include n equal maps.

8. To treat the theory of corresponding lines, we write the equation of a line in any map as

$$\frac{x}{b} + \frac{\bar{x}}{\bar{b}} = 1.$$

This line in M_1 overlies in the reference plane the line

$$\frac{\alpha_1 x_1 - a_1}{b} + \left(\frac{\bar{x}_1}{\alpha_1} - \bar{a}_1\right)\frac{1}{\bar{b}} = 1.$$

Three corresponding lines have an incenter. It is unique for the lines are directed. For the incenter x we have

$$\frac{\alpha_1 x - a_1}{b} + \left(\frac{x}{\alpha_1} - \bar{a}_1\right)\frac{1}{\bar{b}} - 1 = \frac{2\rho}{\sqrt{b\bar{b}}}$$

whence multiplying by $\dfrac{\alpha_1}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)}$, etc., summing and setting $b/\bar{b}$ equal to β

$$(8.1) \qquad x = \sum^{3} (a_1 + \beta \bar{a}_1) \frac{\alpha_1}{(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)}.$$

Here only the direction of the line appears. For naturally the incenter of three directed lines is still the incenter when they are moved through equal distances each to its left, or to its right. When the lines meet at a point, the incenter is that point; thus the incenter is a point on the circle C_{123} on the fixed points.

For four corresponding lines the four incenters lie on the circle

$$(8.2) \qquad x = \sum^{4} (a_1 + \beta \bar{a}_1) \frac{\alpha_1(\alpha_1 - T)}{f'(\alpha_1)}$$

where

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4).$$

If we let

$$c_0 = \sum^{4} \frac{a_1 \alpha_1^2}{f'(\alpha_1)}, \qquad c_1 = \sum^{4} \frac{a_1 \alpha_1}{f'(\alpha_1)}, \qquad c_2 = \sum^{4} \frac{a_1}{f'(\alpha_1)},$$

whence

$$-\bar{c}_0 = \sum^{4} \frac{\bar{a}_1 \sigma_4}{f'(\alpha_1)}, \qquad -\bar{c}_1 = \sum^{4} \frac{\bar{a}_1 \alpha_1 \sigma_4}{f'(\alpha_1)}, \qquad -\bar{c}_2 = \sum^{4} \frac{\bar{a}_1 \alpha_1^2 \sigma_4}{f'(\alpha_1)}.$$

Consequently the equation of the circle (8.2) can be written as

$$(8.3) \qquad x = c_0 - c_1 T - (\beta/\sigma_4)(\bar{c}_2 - \bar{c}_1 T).$$

For varying β we obtain all the circles. As soon as we recognize that the theory of corresponding lines is that of directed lines, we can apply the latter. We know [7] that the incenters of 3/4 lines are on a circle, that the circles for 4/5 lines are the osculants of a cardioid, and so on. Thus the above circles are osculants of a cardioid, and the analysis just indicated is of use only to connect the constants of this line theory with those of the point theory. In the present case the cusp of the cardioid is where four corresponding lines meet at a point—the node of the limaçon.

In the case $c_1 = 0$, the circles all become points; four corresponding lines touch a circle. This happens in general only for the direction given by $c_1 \sigma_4 = \beta \bar{c}_1$. If it should happen for two directions, then $c_1 = 0$ and it always happens.

WESTERN RESERVE UNIVERSITY.

---

[7] F. H. Loud, *Transactions of the American Mathematical Society*, vol. 1 (1900), p. 323.

QUADRIC FIELDS IN THE GEOMETRY OF THE WHIRL-MOTION GROUP G_6.*[1]

By Edward Kasner and John de Cicco.

This paper is a continuation of the paper by the authors entitled "The Geometry of the Whirl-Motion Group G_6, Elementary Invariants," *Bulletin of the American Mathematical Society*, vol. 44 (1938), pp. 399-403. Our main object is to pass from flat fields to quadric fields or differential equations. We develop new aspects of the geometry of differential equations. The present paper can be read without referring to the earlier work.

We begin by considering certain simple transformations on the oriented lineal elements of the plane. A *turn* T_a converts each element into one having the same point and a direction making a fixed angle α with the original direction. By a *slide* S_k the line of the element remains the same and the point moves along the line a fixed distance k. These transformations together generate a continuous group of three parameters, which we call the group of *whirl* transformations W_3. The group of whirls W_3 is isomorphic to the group of rigid motions M_3 and these two groups are commutative and generate a new group of six parameters, which we call the *whirl-motion* group G_6. In the preceding paper, we began a study of the geometry of this group; and in this paper, it is our purpose to continue that study.

A *turbine* consists of the ∞^1 elements whose points lie on a circle (linear or non-linear) and whose directions make a constant angle α with the tangent directions of that circle. A *flat field* consists of the ∞^2 elements which are co-circular with a fixed central element; or, as a special case, of the ∞^2 elements on the ∞^1 straight lines which are parallel and possess the same orientation. Under G_6, turbines and flat fields are transformed into turbines and flat fields.

It is to be observed that there is a larger group G_{15} which converts turbines into turbines (and hence flat fields into flat fields). This group was considered by Kasner in 1911, "The Group of Turns and Slides, and the Geometry of Turbines," *American Journal of Mathematics*, vol. 33. The group G_{15} (which includes Lie's ten-parameter circle group) is most readily handled by means of a certain representation R between the oriented lineal lements of the plane

* Received February 21, 1938.

[1] Presented to the American Mathematical Society, February 1937.

and the points of a projective three-space, in which the turbines and the flat fields of the plane correspond to the straight lines and the planes of the three-space. The fields which by the representation R correspond to the quadric surfaces of the three-space we call the *quadric fields.* It then follows that *under the turbine group* G_{15}, *quadric fields become quadric fields.*

It is the purpose of this paper to study the geometry of the quadric fields relative to the whirl-motion group G_6, which of course is a subgroup of the turbine group G_{15}. We find that *under the whirl-motion group* G_6, *the quadric fields are classified into nine distinct types.* We also find the complete set of invariants of each one of the nine types; the number of invariants may be 0, 1, 2, or 3. The most general type has three invariants.

In this paper we do not attempt to find the integral curves of the nine types of quadric fields, but we will, however, indicate certain interesting special quadric fields whose integral curves are circles:

(1) Quadric fields defined by ∞^1 concentric circles.

(2) Quadric fields defined by the ∞^1 circles tangent to two fixed lines which are not simultaneously parallel and of the same orientation.

(3) Quadric fields defined by the ∞^1 circles tangent to two concentric circles of opposite orientation.

(4) Quadric fields defined by the ∞^1 circles tangent to two distinct circles which are simultaneously congruent and of the same orientation.

(5) Quadric fields defined by the ∞^1 circles tangent to a fixed line and a fixed non-linear circle (*proper or null*) which are not tangent to each other.

(6) Quadric fields defined by the ∞^1 circles tangent to two non-linear circles (*proper or null*) which are neither concentric nor tangent to each other nor simultaneously congruent and of the same orientation.

These six examples of special quadric fields appear under distinct classes or types. The integration of the nine types of differential equations would be interesting; but will be reserved for a later paper.

For the analytic representation, it will be convenient to define an element by the coördinates (u, v, w) where v is the length of the perpendicular from the origin, u is the angle between the perpendicular and the initial line, and w is the distance between the foot of the perpendicular and the point of the element. In our theory we find three coördinate systems useful: (1) the cartesian coördinate system (x, y, y'), (2) the hessian coördinate system (u, v, v'), which we have just defined above, and finally (3) the homogeneous coördinate system (x_1, x_2, x_3, x_4), which is derived from the representation R and is defined by formulas (6) in section 3.

1. The whirl-motion group G_6. A *turn* T_α converts each element of the plane into one having the same point and a direction making a fixed angle α with the original direction. By a *slide* S_k the line of the element remains the same and the point moves along the line a fixed distance k. These transformations together generate a continuous group of three parameters which we call the group of *whirl* transformations W_3. The group of whirls W_3 is isomorphic to the group of rigid motions M_3. These two groups are commutative and together generate a continuous group of six parameters which we call the *whirl-motion* group G_6.

The equations of any whirl-motion transformation are

$$
\begin{aligned}
&\bar{u} = u + \alpha + \lambda,\\
(1)\qquad &\bar{v} = v \cos\alpha + w \sin\alpha + \mu \cos(u+\alpha) + \nu \sin(u+\alpha) + d,\\
&\bar{w} = - v \sin\alpha + w \cos\alpha - \mu \sin(u+\alpha) + \nu \cos(u+\alpha) + k.
\end{aligned}
$$

2. The turbine and the flat field. A *turbine* consists of the ∞^1 elements whose points are on a circle (linear or non-linear) and whose directions make a constant angle α with the directions of that circle. The turbine is called *non-linear* or *linear* according as the base circle is non-linear or linear.

The equations of a non-linear turbine are

$$(2)\qquad v = a\cos u + b \sin u + r, \quad w = -a \sin u + b\cos u + s;$$

and the equations of a linear turbine are

$$(3)\qquad u = u_0 - \alpha, \quad v\cos\alpha + w \sin\alpha = v_0.$$

A *non-linear flat field* consists of the ∞^2 elements which are co-circular with a fixed central element. A *linear flat field* consists of the ∞^2 elements on the ∞^1 straight lines which are parallel and have the same orientation.

The equation of a non-linear flat field is

$$(4)\qquad (v-b)\cos\frac{u-a}{2} - (w+c)\sin\frac{u-a}{2} = 0;$$

and the equation of a linear flat field is

$$(5)\qquad u = \alpha.$$

3. The fundamental representation in space, *R*.[2] The group G_{15} con-

[2] See the discussion given by Kasner in the paper, "The group of turns and slides, and the geometry of turbines," published in the *American Journal of Mathematics*, vol. 33, no. 2 (1911), where the relation to Lie's representation is indicated, Lie-Scheffers, *Berührungtransformationen*, p. 247. Our representation has the advantage of being one-to-one and of applying to all turbines instead of merely to circles.

verting turbines into turbines is most readily handled by means of a certain new set of coördinates for oriented elements, namely

$$(6) \qquad (R) \qquad \begin{aligned} &\rho x_1 = v \cos u/2 - w \sin u/2, \quad \rho x_2 = v \sin u/2 + w \cos u/2, \\ &\rho x_3 = \cos u/2, \quad \rho x_4 = \sin u/2. \end{aligned}$$

The inverse of the transformation (6) is given by the equations

$$(6') \qquad (R^{-1}) \qquad \begin{gathered} u = 2 \operatorname{arc} \tan x_4/x_3, \\ v = \frac{x_1 x_3 + x_2 x_4}{x_3^2 + x_4^2}, \qquad w = \frac{-x_1 x_4 + x_2 x_3}{x_3^2 + x_4^2}. \end{gathered}$$

By the equations (6) and (6′) we see that if we exclude the points of the straight line $x_3 = 0$, $x_4 = 0$ of the three-space, the correspondence between the oriented elements of the plane and the points of the three-space is a continuous one-to-one transformation.

The equations of the non-linear turbine (2) then become

$$(7) \qquad x_1 = (a + r)x_3 + (b - s)x_4, \quad x_2 = (b + s)x_3 + (-a + r)x_4;$$

and the equations of the linear turbine (3) become

$$(8) \qquad \frac{x_1 \cos \dfrac{u_0 + \alpha}{2} + x_2 \sin \dfrac{u_0 + \alpha}{2}}{v_0} = \frac{x_3}{\cos \dfrac{u_0 - \alpha}{2}} = \frac{x_4}{\sin \dfrac{u_0 - \alpha}{2}}.$$

The equation of the non-linear flat field (4) becomes

$$(9) \qquad \begin{aligned} x_1 \cos a/2 + x_2 \sin a/2 - x_3(b \cos a/2 - c \sin a/2) \\ - x_4(b \sin a/2 + c \cos a/2) = 0; \end{aligned}$$

and the equation of the linear flat field (5) becomes

$$(10) \qquad \frac{x_3}{\cos \alpha/2} = \frac{x_4}{\sin \alpha/2}.$$

Thus it is seen that in the new set of coördinates (x_1, x_2, x_3, x_4), which we term the *homogeneous coördinates* of an element, a flat field is given by a linear equation, and a turbine is given by two linear equations.

We may regard (6) and (6′) as establishing a correspondence between the elements (u, v, w) of the plane and the points whose homogeneous coördinates are (x_1, x_2, x_3, x_4) of a projective three-dimensional space. *In this representation, which we designate by R, the ∞^4 turbines of the plane are*

pictured by the ∞^4 *straight lines of space; and the* ∞^3 *flat fields of the plane are pictured by the* ∞^3 *planes of space.*

It follows that element transformations converting turbines into turbines correspond to collineations in space, and hence *constitute a continuous group* G_{15}. Then it is obvious that, under G_{15}, flat fields become flat fields.

4. The quadric fields and the whirl-motion group G_6. The fields which by the representation R correspond to the quadric surfaces of space we call the *quadric fields.*

By equations (6), it is seen that the equation of any quadric field is

$$\begin{aligned} &v^2(A\cos u + B\sin u + C) + w^2(-A\cos u - B\sin u + C) \\ &\quad + 2vw(-A\sin u + B\cos u) + 2v(D\cos u + E\sin u + F) \\ &\quad + 2w(-D\sin u + E\cos u + G) + K\cos u + L\sin u + M = 0. \end{aligned} \tag{11}$$

Under the turbine group G_{15}, the quadric fields are converted into quadric fields; and hence, under the whirl-motion group G_6, which is a subgroup of G_{15}, the quadric fields are converted into quadric fields.

By applying the equations (1) to the equation (11), we find that the equations of the group of the transformations between the quadric fields of the plane, (which is induced by the whirl-motion group G_6), are

$$\begin{aligned} \rho A &= \bar{A}\cos(-\alpha+\lambda) + B\sin(-\alpha+\lambda), \\ \rho B &= -\bar{A}\sin(-\alpha+\lambda) + \bar{B}\cos(-\alpha+\lambda), \\ \rho C &= \bar{C}, \\ \rho D &= \bar{A}\,(d\cos\lambda - k\sin\lambda) + \bar{B}(d\sin\lambda + k\cos\lambda) \\ &\quad + \mu\bar{C} + \bar{D}\cos\lambda + \bar{E}\sin\lambda, \\ \rho E &= \bar{A}(-d\sin\lambda - k\cos\lambda) + \bar{B}(d\cos\lambda - k\sin\lambda) \\ &\quad + \nu\bar{C} - \bar{D}\sin\lambda + \bar{E}\cos\lambda, \\ \rho F &= \bar{A}\{\mu\cos(-\alpha+\lambda) - \nu\sin(-\alpha+\lambda)\} \\ &\quad + \bar{B}\{\mu\sin(-\alpha+\lambda) + \nu\cos(-\alpha+\lambda)\} \\ &\quad + \bar{C}(d\cos\alpha - k\sin\alpha) + \bar{F}\cos\alpha - \bar{G}\sin\alpha, \\ \rho G &= \bar{A}\{-\mu\sin(-\alpha+\lambda) - \nu\cos(-\alpha+\lambda)\} \\ &\quad + \bar{B}\{\mu\cos(-\alpha+\lambda) - \nu\sin(-\alpha+\lambda)\} \\ &\quad + \bar{C}(d\sin\alpha + k\cos\alpha) + \bar{F}\sin\alpha + \bar{G}\cos\alpha, \\ \rho K &= \bar{A}[(\mu^2-\nu^2)\cos(-\alpha+\lambda) - 2\mu\nu\sin(-\alpha+\lambda) \\ &\quad + (d^2-k^2)\cos(\alpha+\lambda) - 2dk\sin(\alpha+\lambda)] \\ &\quad + \bar{B}[(\mu^2-\nu^2)\sin(-\alpha+\lambda) + 2\mu\nu\cos(-\alpha+\lambda) \\ &\quad + (d^2-k^2)\sin(\alpha+\lambda) + 2dk\cos(\alpha+\lambda)] \\ &\quad + \bar{C}[2d(\mu\cos\alpha + \nu\sin\alpha) + 2k(-\mu\sin\alpha + \nu\cos\alpha)] \end{aligned} \tag{12}$$

$$
\begin{aligned}
&+ 2\bar{D}[d \cos(\alpha+\lambda) - k \sin(\alpha+\lambda)] \\
&+ 2\bar{E}[d \sin(\alpha+\lambda) + k \cos(\alpha+\lambda)] + 2\bar{F}(\mu \cos\alpha + \nu \sin\alpha) \\
&+ 2\bar{G}(-\mu \sin\alpha + \nu \cos\alpha) + \bar{K} \cos(\alpha+\lambda) + \bar{L} \sin(\alpha+\lambda), \\
\rho L = {} & \bar{A}[(\mu^2-\nu^2) \sin(-\alpha+\lambda) + 2\mu\nu \cos(-\alpha+\lambda) \\
&- (d^2-k^2) \sin(\alpha+\lambda) - 2dk \cos(\alpha+\lambda)] \\
&+ \bar{B}[-(\mu^2-\nu^2) \cos(-\alpha+\lambda) + 2\mu\nu \sin(-\alpha+\lambda) \\
&+ (d^2-k^2) \cos(\alpha+\lambda) - 2dk \sin(\alpha+\lambda)] \\
&+ \bar{C}[2d(-\mu \sin\alpha + \nu \cos\alpha) + 2k(-\mu \cos\alpha - \nu \sin\alpha)] \\
&+ 2\bar{D}[-d \sin(\alpha+\lambda) - k \cos(\alpha+\lambda)] \\
&+ 2\bar{E}[d \cos(\alpha+\lambda) - k \sin(\alpha+\lambda)] \\
&+ 2\bar{F}(-\mu \sin\alpha + \nu \cos\alpha) + 2\bar{G}(-\mu \cos\alpha - \nu \sin\alpha) \\
&- \bar{K} \sin(\alpha+\lambda) + \bar{L} \cos(\alpha+\lambda), \\
\rho M = {} & \bar{A}[2d(\mu \cos\lambda - \nu \sin\lambda) + 2k(-\mu \sin\lambda - \nu \cos\lambda)] \\
&+ \bar{B}[2d(\mu \sin\lambda + \nu \cos\lambda) + 2k(\mu \cos\lambda - \nu \sin\lambda)] \\
&+ \bar{C}(\mu^2+\nu^2+d^2+k^2) + 2\bar{D}(\mu \cos\lambda - \nu \sin\lambda) \\
&+ 2\bar{E}(\mu \sin\lambda + \nu \cos\lambda) + 2\bar{F}d + 2\bar{G}k + \bar{M}.
\end{aligned}
$$

5. The nine classes of quadric fields. From (12) we find that *under the whirl-motion group G_6, the quadric fields can be classified into nine distinct classes.* These nine classes will be denoted by the Greek letters $\alpha, \beta, \gamma, \delta, \epsilon, \zeta, \eta, \theta, \pi$. The discussion is very complicated and will not be given here in detail. The results are merely stated.

The α-quadric field. Any quadric field whose equation is of the form

$$K \cos u + L \sin u + M = 0, \tag{13}$$

where $K^2 + L^2 \neq 0$ is called an α-quadric field.

It is found that, *under G_6, any α-quadric field becomes an α-quadric field, and it has the unique invariant*

$$\frac{M^2}{K^2 + L^2}. \tag{14}$$

Any α-quadric field consists of two linear flat fields, that is, it is composed of the ∞^2 elements on two parallel sets of oriented lines.

The canonical form of an α-quadric field is

$$\cos u + M = 0. \tag{13'}$$

The β-quadric field. Any quadric field whose equation is of the form

$$2Fv + 2Gw + K \cos u + L \sin u + M = 0, \tag{15}$$

where $F^2 + G^2 \neq 0$ is called a *β-quadric field.*

It is found that, *under G_6, any β-quadric field becomes a β-quadric field, and that it has no invariants.*

The canonical form of a β-quadric field is

$$v = 0. \tag{15'}$$

The β-qadric field (15′) *consists of the ∞^2 elements on the ∞^1 straight lines through the origin.*

In the class of β-quadric fields are included the fields whose integral curves consist of ∞^1 concentric circles; or of the ∞^1 straight lines tangent to a fixed circle (proper or null).

The γ-quadric field. Any quadric field whose equation is of the form

$$\begin{aligned} 2v(D\cos u + E\sin u + F) + 2w(-D\sin u + E\cos u + G) \\ + K\cos u + L\sin u + M = 0, \end{aligned} \tag{16}$$

where $D^2 + E^2 = F^2 + G^2 \neq 0$ is called a *γ-quadric field.*

It is found that, *under G_6, any γ-quadric field becomes a γ-quadric field and it has the unique invariant*

$$\frac{\left[\dfrac{D(FK - GL) + E(GK + LF)}{F^2 + G^2} - M\right]^2}{F^2 + G^2}. \tag{17}$$

The canonical form of a γ-quadric field is

$$2v(1 + \cos u) - 2w\sin u + M = 0. \tag{16'}$$

It is seen that *if the invariant* (17) *is zero, then the γ-quadric field consists of a linear flat field and a non-linear flat field.*

Thus in the class of γ-quadric fields are included the fields whose integral curves consist of the ∞^1 circles which contain a fixed central element and also ∞^1 parallel straight lines.

The δ-quadric field. Any quadric field whose equation is of the form

$$\begin{aligned} 2v(D\cos u + E\sin u + F) + 2w(-D\sin u + E\cos u + G) \\ + K\cos u + L\sin u + M = 0, \end{aligned} \tag{18}$$

where $F^2 + G^2 \neq D^2 + E^2 \neq 0$ is called a *δ-quadric field.*

It is found that, *under G_6, any δ-quadric field becomes a δ-quadric field and it has the unique invariant*

$$\frac{F^2 + G^2}{D^2 + E^2}. \tag{19}$$

The canonical form of the δ-quadric field is

$$v \cos u + w(-\sin u + G) = 0, \tag{18'}$$

where $G \neq \pm 1$. *The δ-quadric field* (18′) *consists of the ∞^1 circles which are tangent to the two straight lines*

$$u = -\operatorname{arc}\sin G, \quad v = 0.$$

Thus in the class of δ-quadric fields are included the fields whose integral curves consist of the ∞^1 circles tangent to two fixed oriented lines which are not parallel.

The ϵ-quadric field. Any quadric field whose equation is of the form

$$\begin{aligned} v^2 + w^2 + 2v(D\cos u + E\sin u + F) \\ + 2w(-D\sin u + E\cos u + G) + K\cos u + L\sin u + M = 0, \end{aligned} \tag{20}$$

is called an *ϵ-quadric field.*

It is found that, *under G_6, any ϵ-quadric field becomes an ϵ-quadric field, and it has the two fundamental invariants*

$$(K - 2DF - 2EG)^2 + (L + 2DG - 2EF)^2, \tag{21}$$

and

$$-M + D^2 + E^2 + F^2 + G^2. \tag{22}$$

The canonical form of the ϵ-quadric fields is

$$v^2 + w^2 + K\cos u + M = 0. \tag{20'}$$

It is found that *if the invariant* (21) *is zero, then the ϵ-quadric field consists of all the elements which are at a constant distance from a fixed turbine.* (See the preceding paper.)

It is seen that *in the class of ϵ-quadric fields are included the fields whose integral curves are the ∞^1 circles tangent to two concentric circles of opposite orientation. The centers of the circles then are on a circle concentric with the two fixed circles and whose radius is one-half the difference of the two given radii.*

The ζ-quadric field. Any quadric field whose equation is of the form

$$\begin{aligned}(23)\qquad &(v^2 - w^2)(A\cos u + B\sin u) + 2vw(-A\sin u + B\cos u)\\ &+ 2v(D\cos u + E\sin u + F) + 2w(-D\sin u + E\cos u + G)\\ &+ K\cos u + L\sin u + M = 0,\end{aligned}$$

where $A^2 + B^2 \neq 0$ *is called a ζ-quadric field.*

It is found that, *under G_6, any ζ-quadric field becomes a ζ-quadric field, and it has the two fundamental invariants*

$$(24)\qquad \frac{\left\{\begin{aligned}&\left[K + \frac{-A(D^2 - E^2) - 2BDE - A(F^2 - G^2) - 2BFG}{A^2 + B^2}\right]^2\\ &+\left[L + \frac{-2ADE + B(D^2 - E^2) + 2AFG - B(F^2 - G^2)}{A^2 + B^2}\right]^2\end{aligned}\right\}}{A^2 + B^2},$$

and

$$(25)\qquad \frac{\left[M + \frac{-2D(AF + BG) - 2E(-AG + BF)}{A^2 + B^2}\right]^2}{A^2 + B^2}.$$

The canonical form of the ζ-quadric field is

$$(23')\qquad (v^2 - w^2)\cos u - 2vw\sin u + K\cos u + M = 0.$$

It is observed that *if the invariants* (24) *and* (25) *are both zero, the ζ-quadric field consists of two non-linear flat fields such that the angle between them is π.*

In the ζ-quadric fields are included those fields whose integral curves are the ∞^1 circles tangent to two distinct circles which are simultaneously congruent and of the same orientation. Then the centers of the circles are on the straight line which is the perpendicular bisector of the segment joining the centers of the two fixed circles.

The η-quadric field. Any quadric field whose equation is of the form

$$\begin{aligned}(26)\qquad &v^2(A\cos u + B\sin u + 1) + w^2(-A\cos u - B\sin u + 1)\\ &\qquad + 2vw(-A\sin u + B\cos u)\\ &+ 2v(D\cos u + E\sin u + F) + 2w(-D\sin u + E\cos u + G)\\ &\qquad + K\cos u + L\sin u + M = 0,\end{aligned}$$

where

$$\begin{aligned}(27)\qquad &A^2 + B^2 = 1,\\ &F = AD + BE, \quad G = -AE + BD,\end{aligned}$$

is called an *η-quadric field.*

It is found that, *under G_6, any η-quadric field becomes an η-quadric field, and that it has the two fundamental invariants*

$$(28)\quad [K - A(D^2 - E^2) - 2BDE]^2 + [L - 2ADE + B(D^2 - E^2)]^2,$$

and

$$(29)\quad -M + D^2 + E^2.$$

The canonical form of the η-quadric field is

$$(26')\quad v^2(1 + \cos u) + w^2(1 - \cos u) - 2vw \sin u + K \cos u + M = 0.$$

If the invariant (28) *is zero, then the η-quadric field becomes a spherical field. A spherical field consists of the elements which are at a constant distance from a fixed flat field* (*see the preceding paper*).

The spherical field is important in the differential geometry of element series. (See the abstract, "The Inverse of Meusnier's Theorem in the Geometry of Element Series," by De Cicco, which was presented to the American Mathematical Society in December, 1937).

If the invariants (28) *and* (29) *are both equal, then the η-quadric field consists of two parallel non-linear flat fields.*

Thus in the class of η-quadric fields are included the fields whose integral curves consist of the $2\infty^1$ circles which contain two fixed parallel elements.

The θ-quadric field. Any quadric field whose equation is of the form

$$(30)\quad \begin{aligned} v^2(A \cos u + B \sin u + 1) + w^2(-A \cos u - B \sin u + 1) \\ + 2vw(-A \sin u + B \cos u) \\ + 2v(D \cos u + E \sin u + F) + 2w(-D \sin u + E \cos u + G) \\ + K \cos u + L \sin u + M = 0, \end{aligned}$$

where

$$A^2 + B^2 = 1,$$

$$(31)\quad D^2 + E^2 + F^2 + G^2 - 2A(DF - EG) - 2B(DG + EF) \neq 0,$$

is called a *θ-quadric field.*

It is found that, *under G_6, any θ-quadric field becomes a θ-quadric field, and it has the two fundamental invariants*

$$(32)\quad D^2 + E^2 + F^2 + G^2 - 2A(DF - EG) - 2B(DG + EF),$$

and

$$
\begin{aligned}
(33)\quad & M + D^2 + E^2 + F^2 + G^2 \\
& + \frac{\left\{\begin{aligned}
&+K\{A(F^2-G^2)+2BFG+A(D^2-E^2)+2BDE-2(DF+EG)\}\\
&-L\{-B(F^2-G^2)+2AFG+B(D^2-E^2)-2ADE-2(DG-EF)\}\\
&+(A^2-B^2)(D^2-E^2)(F^2-G^2)-4DEFG(A^2-B^2)\\
&+4ABFG(D^2-E^2)+4ABDE(F^2-G^2)\\
&-(D^2+E^2)^2-(F^2+G^2)^2+(D^2+E^2)(F^2+G^2)
\end{aligned}\right\}}{D^2+E^2+F^2+G^2-2A(DF-EG)-2B(DG+EF)}.
\end{aligned}
$$

The canonical form of the θ-quadric field is

$$
(30')\quad \begin{aligned} & v^2(1+\cos u) + w^2(1-\cos u) - 2vw\sin u \\ & \quad + 2Dv\cos u - 2Dw\sin u + M = 0, \end{aligned}
$$

where $D \neq 0$.

In the θ-quadric fields are included the fields whose integral curves consist of the ∞^1 circles tangent to a fixed line and a fixed non-linear circle (proper or null) which are not tangent to each other. Then the centers of the circles are on the parabola whose focus is the center of the fixed circle and whose directrix is parallel to the fixed line in such a way that the distance from the fixed line to the directrix is the radius of the fixed circle.

The π-quadric field. Any quadric field whose equation is of the form

$$
(34)\quad \begin{aligned} & v^2(A\cos u + B\sin u + 1) + w^2(-A\cos u - B\sin u + 1) \\ & \quad + 2vw(-A\sin u + B\cos u) \\ & + 2v(D\cos u + E\sin u + F) + 2w(-D\sin u + E\cos u + G) \\ & \quad + K\cos u + L\sin u + M = 0, \end{aligned}
$$

where $A^2 + B^2 \neq 0, 1$ is called a *π-quadric field.*

It is found that, *under G_6, any π-quadric field becomes a π-quadric field, and it has the three fundamental invariants*

$$
(35)\quad A^2 + B^2,
$$

and

$$
\begin{aligned}
(36)\quad & \left[-K + \frac{A(D^2-E^2)+2BDE+A(F^2-G^2)+2BFG-2(DF+EG)}{A^2+B^2-1}\right]^2 \\
& + \left[-L + \frac{-B(D^2-E^2)+2ADE+B(F^2-G^2)-2AFG+2(DG-EF)}{A^2+B^2-1}\right]^2,
\end{aligned}
$$

and

$$
(37)\quad M + \frac{D^2+E^2+F^2+G^2-2A(DF-EG)-2B(DG+EF)}{A^2+B^2-1}.
$$

The canonical form of the π-quadric field is

$$v^2(A\cos u + 1) + w^2(-A\cos u + 1) - 2Avw\sin u + K\cos u + M = 0, \tag{34'}$$

where $A \neq 0, \pm 1$.

It is noted that, *if the invariants* (36) *and* (37) *are both zero, then the π-quadric consists of two non-linear flat fields in such a way that the angle between them is* not 0 *or π.*

In the π-quadric fields are included the fields whose integral curves consist of the ∞^1 circles tangent to two non-linear circles (proper or null) which are neither concentric nor tangent to each other nor simultaneously congruent and of the same orientation. Then the centers of the circles are on a central conic (not a circle) whose foci are the centers of the two fixed circles and whose semi major axis is one-half the difference of the two given radii.

In this paper we have given the complete analytic classification into nine distinct types, and we have given the complete set of invariants of each type. It remains to discover the geometric construction of each type, and the geometric interpretation of the invariants.

COLUMBIA UNIVERSITY,
AND
BROOKLYN COLLEGE.

MEAN MOTION. II.*

By Hermann Weyl.

In order to establish "*mean motion*" for the azimuth ϕ of a finite exponential sum

$$(1) \qquad z = r \cdot e(\phi) = \sum_{k=1}^{n} a_k \cdot e(\theta_k),$$

$$(2) \qquad \theta_k = \theta_k{}^0 + \lambda_k t,$$

in which the amplitudes a_k are arbitrary complex constants while the frequencies λ_k and phases θ_k, $\theta_k{}^0$ are real, one has to resort to the Kronecker equidistribution law for the straight line (2) in the n-dimensional torus space $(\theta_1, \cdots, \theta_n)$. The time t is a real variable. The result derived in a previous paper of mine [1], for the case of a "totally irrational" frequency vector $\lambda = (\lambda_1, \cdots, \lambda_n)$, is independent of the initial phases $\theta_k{}^0$. The first remark which I wish to add here is to the effect that the limit of $\phi(t)/t$ defining the mean motion exists *uniformly* with respect to the $\theta_k{}^0$. This is an immediate consequence of the transcendental method based on finite Fourier series by which I proved the equidistribution law. For certain singular values of the initial phases $\theta_k{}^0$ the curve $z = z(t)$ will pass through the origin and thereby cause ambiguity of the continuation of $\phi(t)$. In the most effective way our uniformity silences these trouble makers by embedding them in the army of all possible initial phases.

In the second place I propose to study the case where λ is not totally irrational. As often happens, the whole treatment becomes considerably more satisfactory and natural if one is forced to include the "exceptions." The wholesome influence in this case comes from the necessity of stating the problem in terms of an arbitrary lattice basis. In the n-dimensional space of the vectors $\xi = (\xi_1, \cdots, \xi_n)$ all the equations with integral coefficients h,

$$(3) \qquad h_1\xi_1 + \cdots + h_n\xi_n = 0,$$

satisfied by $\lambda = (\lambda_1, \cdots, \lambda_n)$ define a linear subspace E of dimensionality $m \leqq n$. As one readily sees, E is a *lattice subspace*, i. e. we can find m linearly independent lattice vectors in E,

$$\mathfrak{l}_1 = (l_{11}, \cdots, l_{1n}), \cdots, \mathfrak{l}_m = (l_{m1}, \cdots, l_{mn})$$

* Received November 18, 1938.

(lattice basis) such that a vector

$$\xi = \xi'_1 \mathfrak{l}_1 + \cdots + \xi'_m \mathfrak{l}_m \tag{4}$$

in E is a lattice vector (namely a vector with integral components ξ_k) if and only if the ξ'_i are integers. Hence by identifying points on E whose difference is a lattice vector, E is changed into an m-dimensional torus space (E). We call ξ *totally irrational* in E if the components ξ'_i are linked by no homogeneous linear relation with integral coefficients. This notion is clearly independent of the choice of the lattice basis $\mathfrak{l}_i$, and λ itself is totally irrational in E. In agreement with (4) we set

$$\lambda = \lambda'_1 \mathfrak{l}_1 + \cdots + \lambda'_m \mathfrak{l}_m.$$

We apply our former method to the function $z(\theta'_1, \cdots, \theta'_m)$ arising from (1) by the substitution

$$\theta = \theta'_1 \mathfrak{l}_1 + \cdots + \theta'_m \mathfrak{l}_m \quad \text{or} \quad \theta_k = l_{1k}\theta'_1 + \cdots + l_{mk}\theta'_m.$$

In this function we have to set

$$\theta'_k = \lambda'_k t \text{ or more generally } \theta'_k = \theta'^0_k + \lambda'_k t.$$

The azimuth of the resulting function $z(t)$ has a mean motion M expressible as a certain volume or flux. Namely, one "slits" (E) in the locus of those points θ in E for which (1) is real and negative, and for an arbitrary vector ξ in E one determines the flux $W(\xi)$ sent through the slit by the constant current of velocity $\xi = (\xi_1, \cdots, \xi_n)$. Then the mean motion $M = W(\lambda)$.

The flux $W(\xi)$ considered as a function of the variable vector (4) has quite remarkable properties. By its very definition it is *independent of the choice of the lattice basis* $\mathfrak{l}_1, \cdots, \mathfrak{l}_m$ *in* E. Moreover it is *a linear form in* E. Let us therefore write

$$W(\xi) = W'_1 \xi'_1 + \cdots + W'_m \xi'_m. \tag{6}$$

For given values $\theta'_2, \cdots, \theta'_m$ and with the parameter θ'_1 traveling over a full cycle from 0 to 1, $z(\theta'_1, \cdots, \theta'_m)$ describes a closed curve $C(\theta'_2, \cdots, \theta'_m)$. The coefficient W'_1 is given by the integral

$$\int_0^1 \cdots \int_0^1 N(\theta'_2, \cdots, \theta'_m)\, d\theta'_2 \cdots d\theta'_m$$

where N denotes the number of times this curve $C(\theta'_2 \cdots \theta'_m)$ surrounds the origin. I transform the expression for W'_1 to which our method immediately

leads by a very simple trick. If $\theta'_1, \cdots, \theta'_m$ are fixed and t is the variable parameter, then

$$z = z(t + \theta'_1, \theta'_2, \cdots, \theta'_m)$$

describes a curve $C(\theta'_1, \cdots, \theta'_m)$ which is actually independent of θ'_1 and coincides with $C(\theta'_2, \cdots, \theta'_m)$. If it surrounds the origin $N(\theta'_1, \theta'_2, \cdots, \theta'_m)$ times, one has

$$W'_1 = \int_0^1 \cdots \int_0^1 N(\theta'_1, \cdots, \theta'_m)\, d\theta'_1 \cdots d\theta'_m.$$

The argument θ'_1 is a fake. However, in this more symmetric form we can at once get rid of the particular coördinate system $\mathfrak{l}_i$. Considering the fact that $W(\xi)$ has a significance independent of that coördinate system, and that any primitive lattice vector $\mathfrak{l} = (l_1, \cdots, l_n)$ in E (l_k integers without common divisor) may serve as the first basis vector in an appropriate lattice basis for E, we obtain the following definition of the linear form $W(\xi)$ in E.

Denote for any lattice vector $\mathfrak{l}$ in E and any vector θ in E, by $N(\mathfrak{l}; \theta)$ the number of times the curve

$$(7) \qquad C(\mathfrak{l}; \theta): \quad z = \sum_k a_k \cdot e(\theta_k + l_k t) \qquad (0 \leqq t \leqq 1)$$

surrounds the origin. Then

$$(8) \qquad W(\mathfrak{l}) = E_\theta\{N(\mathfrak{l}; \theta)\}.$$

E_θ indicates the average with respect to θ over the m-dimensional torus space (E). The assumption that the l_k are without common divisor may be at once removed since the curve $C(h\mathfrak{l})$, h a positive integer, is h times the curve $C(\mathfrak{l})$. When one has to define a linear form in a lattice subspace without prejudicing the choice of the basis, it is best to give its values for all lattice vectors. In doing so one is obliged to show that these values fit together. Here we have got around that difficulty by means of the invariantive significance of the form (6) as a volume or flux.

The final result becomes perhaps more intelligible if looked at in the following way. If λ (in E) is rational, then it is trivial that

$$(9) \qquad z = \sum_k a_k \cdot e(\theta_k + \lambda_k t)$$

has a mean motion, because the curve is closed. Yet its mean motion is highly sensitive to variation of the initial phases θ_k, and such a simple result as a linear form $W(\lambda)$ is to be expected only after averaging over θ in (E). However, if λ is totally irrational, the curve itself according to the equidistribution

law takes care of this smearing effect and has therefore a mean motion equalling $W(\lambda)$ and independent of θ.

Replacing $e(t)$ in (7) by a complex variable ζ, one can describe $N(\mathfrak{l};\theta)$ as the total order (number of zeros minus number of poles) of the function

$$\sum_k a_k e(\theta_k)\cdot\zeta^{l_k}$$

within the unit circle $|\zeta|<1$. Hence $W(\mathfrak{l})$ lies between the least and the greatest of the components l_k. Approximating to an arbitrary vector (4) in E by such vectors with rational components ξ'_i, one extends this result to all ξ:

The linear form $W(\xi)$ defined on E lies between the least and the greatest of the n components ξ_k of $\xi=(\xi_1,\cdots,\xi_n)$. It is thus characterized as a certain mean value of the components.

Our whole treatment calls for an improvement by taking notice of the equation

$$\phi(\theta_1+\theta,\cdots,\theta_n+\theta)=\phi(\theta_1,\cdots,\theta_n)+\theta$$

and the resulting redundance of one of the phases θ_k. We now define E by all those relations (3) with integral coefficients h for which

$$h_1\lambda_1+\cdots+h_n\lambda_n=0 \quad\text{and}\quad h_1+\cdots+h_n=0.$$

E contains the vector $\mathfrak{e}=(1,1,\cdots,1)$. We determine a lattice basis $\mathfrak{l}_1,\cdots,\mathfrak{l}_m$ of E with $\mathfrak{l}_1=\mathfrak{e}$. By operating in the $(m-1)$-dimensional subspace E^* of E spanned by $\mathfrak{l}_2,\cdots,\mathfrak{l}_m$ we find a mean motion

$$M=\lambda'_1+(W'_2\lambda'_2+\cdots+W'_m\lambda'_m), \tag{10}$$

and for any lattice vector $\mathfrak{l}=l'_2\mathfrak{l}_2+\cdots+l'_m\mathfrak{l}_m$ in E, $W'_2l'_2+\cdots+W'_ml'_m$ is expressed as a certain integral over $\theta'_2,\cdots,\theta'_m$. However, since, in an easily understandable notation, the curve $C(\theta'_1\theta'_2\cdots\theta'_m)$ arises from $C(0\,\theta'_2\cdots\theta'_m)$ by rotating it around the origin by the angle θ'_1, one falls back on the old expression (8):

$$W(\mathfrak{l})=W'_2l'_2+\cdots+W'_ml'_m \qquad (\mathfrak{l}\text{ in }E^*).$$

Moreover, the definition of $N(\mathfrak{l})$ shows readily that

$$N(\mathfrak{l}+l\mathfrak{e})=N(\mathfrak{l})+l \qquad (l\text{ any integer}),$$

and hence for *any* lattice vector $\mathfrak{l}$ in E:

$$W(\mathfrak{l})=l'_1+(W'_2l'_2+\cdots+W'_ml'_m), \tag{11}$$

in particular $W(e) = 1$. Comparison of (10) with (11) reestablishes our former results.

It appears very natural to express the number N in the Cauchy manner:

$$N(\mathrm{I};\theta) = \int_0^1 \Re\left\{\frac{1}{2\pi i}\cdot\frac{z'}{z}\right\}dt;$$

z is again defined by (7), z' is its derivative with respect to t. Hence

$$W(\mathrm{I}) = E_\theta\left\{\int_0^1 \Re\left(\frac{1}{2\pi i}\cdot\frac{z'}{z}\right)dt\right\}.$$

$$\frac{1}{2\pi i}\cdot\frac{z'}{z} = \sum_k l_k\cdot\frac{a_k e(\theta_k + l_k t)}{z}.$$

If one exchanges the integration E_θ and the integration with respect to t, one finds that

$$W(\mathrm{I}) = \sum_k l_k \int_0^1 W_k(t)\,dt$$

with

$$W_k(t) = E_\theta\left\{\frac{a_k e(\theta_k + l_k t)}{z}\right\}.$$

$W_k(t)$ is clearly independent of t. Indeed, I is in E and thus for a given t, $\theta_k \to \theta_k + l_k t$ indicates merely a parallel displacement of E into itself. Therefore

$$W(\mathrm{I}) = \sum_k W_k l_k$$

with

$$W_k = E_\theta\left\{\frac{a_k e(\theta_k)}{a_1 e(\theta_1) + \cdots + a_n e(\theta_n)}\right\}.$$

These formulas are in keeping with the Hartman-van Kampen-Wintner approach [2] and furnish another proof of the fact that $W(\mathrm{I})$ depends linearly on I. The argument hinges, however, on the exchange of two integrations, which is somewhat awkward to justify in view of the infinities of the integrand. I therefore prefer the method here adopted, resting on the simple fact that the flux of a constant current of arbitrary velocity through a given hole depends linearly on the velocity.

We summarize:

Let n real frequencies λ_k and n complex amplitudes a_k be given. All equations $h_1\xi_1 + \cdots + h_n\xi_n = 0$ with integral coefficients h satisfying the relations

$$h_1 + \cdots + h_n = 0, \qquad h_1\lambda_1 + \cdots + h_n\lambda_n = 0$$

define an m-dimensional linear subspace E in the n-space of the generic vector $\xi = (\xi_1, \cdots, \xi_n)$. *The vector* $\mathfrak{e} = (1, 1, \cdots, 1)$ *lies in E. We assume that* $\Sigma a_k \cdot e(\theta_k)$ *does not vanish identically with* $\theta = (\theta_1, \cdots, \theta_n)$ *running over E. Denote for any lattice vector* $\mathfrak{l}$ *in E and any vector* θ *in E by* $N(\mathfrak{l}; \theta)$ *the number of times the curve*

$$z = \sum_k a_k \cdot e(\theta_k + l_k t) \qquad (0 \leqq t \leqq 1)$$

surrounds the origin. There exists a linear form $W(\xi)$ *on E such that for any lattice vector* $\mathfrak{l}$ *in E,*

$$W(\mathfrak{l}) = E_\theta\{N(\mathfrak{l}; \theta)\}.$$

$W(\mathfrak{e}) = 1$. $W(\xi)$ *is* $\geqq 0$ *if all components* ξ_k *of* ξ *are* $\geqq 0$. *The azimuth of*

$$z = \sum_k a_k \cdot e(\theta_k + \lambda_k t)$$

has a mean motion, uniformly with respect to and independent of the initial phases θ_k, *provided the phase vector* $\theta = (\theta_1, \cdots, \theta_n)$ *lies in E. The mean motion equals* $W(\lambda)$.

THE INSTITUTE FOR ADVANCED STUDY,
PRINCETON, N. J.

REFERENCES.

[1] See *American Journal of Mathematics,* vol. 60 (1938), p. 889. Professor Norbert Wiener told me that he and Professor Aurel Wintner have found another way of establishing the general formula for mean motion.

[2] Cf. *American Journal of Mathematics*, vol. 59 (1937), p. 261.

SUR LES THÉORÈMES DE RÉCURRENCE DANS LA DYNAMIQUE GÉNÉRALE.*

par HEINRICH HILMY.

Introduction.

1. Dans le mémoire présent je donne l'analyse logique des théorèmes de récurrence de la théorie générale des systèmes dynamiques: précisement du "Wiederkehrsatz" de Poincaré-Carathéodory et d'un des théorèmes de G. D. Birkhoff sur les mouvements centrals. Je demontre qu'en généralisant convenablement le "Wiederkehrsatz" d'une part et en précisant le théorème de récurrence de G. D. Birkhoff d'autre part, on obtient deux théorèmes qui sont dual par leurs énoncés et les méthodes de leurs démonstration. Il est a remarquer que mon énoncé du théorème de Poincaré-Carathéodory est reversible.

Enfin, je construit des exemples qui éclaircissent l'etendue logique de la classe des systèmes dynamique auxquels sont applicables les deux théorèmes mentionnés.

2. Considérons les mouvements des points p dans l'espace métrique M. Nous désignons par $\rho(p, q)$ la distance entre les points p et q dans l'espace M et par $S(p, \epsilon)$ le voisinage sphérique du point p du rayon ϵ. Nous supposons ensuite que l'espace M est un espace métrique complet.[1] Nous supposons en outre, qu'il existe dans une base dénombrable de domaines, c'est-à-dire qu'il existe un ensemble dénombrable de domaine $U_1, U_2, \cdots, U_n, \cdots$ tel que pour tout point $p \subset M$ et pour tout voisinage sphérique S de ce point il y a un domaine satisfaisant à la condition: $p \subset U_\nu \subset S$. Nous supposons enfin que, dans l'espace M il existe une mesure possédant les propriétés générales de la mesure de Lebesgue et telle qu'on a mes $G > 0$ si G est un ensemble ouvert.

Désignons par $f(p, t)$ la position du point $p \subset M$ à l'instant t du temps; $f(p, 0) = p$. Admettons, de plus qu'on a $f[f(p, t), \tau] = f(p, t + \tau)$. L'ensemble $\{f(p, t)\}$ de tous les points de la forme $f(p, t)$ avec p fixe et avec t variable toutes les valeurs réelles est nommé trajectoire et le point p est le point initial de cette trajectoire.

Admettons que, dans notre cas, a lieu la dépendence continue de la tra-

---

* Received January 10, 1938.

[1] La suite des points $p_1, p_2, \cdots, p_n, \cdots$ est dite suite fondamentale ou suite de Cauchy si pour tout $\epsilon > 0$ il existe un m tel que $\rho(p_n, p_m) < \epsilon$ dès que $n > m$. L'espace où chaque suite fondamentale est convergente s'appelle espace complet.

jectoire des conditions initiales, c'est-à-dire que, pour tout point fixe p, et pour tout couple de nombres positifs et ϵ, T on peut indiquer un nombre positif δ assez petit pour que l'inégalité

$$\rho(f(p,t),f(q,t)) < \epsilon$$

soit vérifiée des que $|t| \leq T$ pourvu que $\rho(p,q) < \delta$.

A étant un sous-ensemble arbitraire de M, nous désignons par $f(A,t)$ l'ensemble des points de la forme $f(p,t)$, où $p \subset A$ et t reste le même pour tout $p \subset A$. Nous dirons que l'ensemble A est un ensemble récurrent pour $t \to +\infty$ ($t \to -\infty$) si, pour tout nombre positif T, on peut indiquer une valeur de t positive (négative) satisfaisant à l'inégalité $|t| > T$ et telle que les ensembles A et $f(A,t)$ ont une partie commune non vide. Dans le cas contraire, si l'on peut indiquer un nombre τ positif (négatif) tel que $f(A,t) \cdot A = 0$ pour tout $t \geqq \tau$ (pour tout $t \leqq \tau$), nous dirons que l'ensemble A est un ensemble érrant pour tout $t \to +\infty$ (pour $t \to -\infty$).

Le mouvement $f(p,t)$ est dit positivement (négativement) stable au sens de Poisson si l'on peut indiquer, pour les nombres arbitraires $\epsilon > 0$ et $T > 0$, des valeurs de t positives (négatives) satisfaisant à l'inégalité $|t| > T$ et telles que

$$\rho(p,f(p,t)) < \epsilon.$$

Le mouvement est dit stable au sens de Poisson, s'il est simultanement positivement et négativement stable dans le même sens.

I.

3. Dans l'espace M où un système dynamique est défini nous définissons une fonction $\Phi(p)$ du point p de cet espace qui caractérise, dans quelque mesure, les mouvements du système dynamique pour le temps changeant dans le sens positif (négatif).

Nous posons $\Phi(p) = 0$ si le point p est situé sur la trajectoire du mouvement positive (négativement) stable au sens de Poisson. Si, au contraire le point p est situé sur la trajectoire d'un mouvement positivement (négativement) instable au sens de Poisson, il existe toujours un nombre $\epsilon > 0$ pour lequel on peut indiquer un nombre positif $\tau = \tau(\epsilon)$ tel que $f(p,t) \not\subset S(p,\epsilon)$ pour tout $|t| > \tau$. Considérons l'ensemble de tous les nombres qui représentent les rayons des voisinages sphériques de p, possédant cette propriété; si cet ensemble a une borne supérieur η nous posons $\Phi(p) = \eta$; dans le cas contraire, nous posont $\Phi(p) = +\infty$.

Nous dirons que la fonction $\Phi(p)$ est la fonction caractéristique du système dynamique pour le temps croissant (décroissant).

4. Dans nos démonstrations des théorèmes concernant les fonctions caractéristiques, nous nous bornerons toujours à l'étude des fonctions définies pour le temps croissant, vu que les démonstrations pour le temps décroissant ne demandent aucune modification essentielle.

THÉORÈME I. *L'ensemble D_η de tous les points $p \subset M$ satisfaisant à la condition $\Phi(p) < \eta$ est un ensemble du type G_δ selon la classification de F. Hausdorff, c'est-à-dire que, cet ensemble est la partie commune d'une suite dénombrable d'ensembles ouverts.*

Prenons une suite de nombres positifs croissant indéfiniment

$$\tau_1, \tau_2, \cdots, \tau_n, \cdots.$$

Désignons par $D_\eta{}^m$ l'ensemble des points $p \subset M$ pour lesquels on peut indiquer un $\tau > \tau_m$, tel que $\rho(p, f(p, \tau)) < \eta$.

Soit p' un point de l'ensemble $D_\eta{}^m$ et soit $\rho(p', f(p', \tau)) = \beta < \eta$.

Choisissons un nombre positif $\epsilon < \frac{1}{2}(\eta - \beta)$ et un nombre $\delta > 0$ assez petit pour que l'inégalité $\rho(f(p', t), f(q, t)) < \epsilon$ soit vérifiée pour tout $|t| \leq \tau$ pourvu que $\rho(p', q) < \delta$, un tel nombre existant en vertu de la dépendance continue des trajectoires des conditions initiales. Alors,

$$\begin{aligned} &\rho(q, p') < \delta \leq \epsilon < \tfrac{1}{2}(\eta - \beta) \\ &\rho(p', f(p', \tau)) = \beta \\ &\rho(f(p', \tau), f(q, \tau)) < \epsilon < \tfrac{1}{2}(\eta - \beta) \end{aligned}$$

d'où, en vertu de l'axiome du triangle, nous avons

$$\rho(q, f(q, \tau)) < \eta$$

Ceci revient à ce que $p' \subset D_\eta{}^m$, $S(p', \epsilon) \subset D_\eta{}^m$ ou à ce que est un ensemble ouvert. Il est aisé de voir que

$$D_\eta = \prod_{i=1}^{\infty} D_\eta{}^i$$

ce qui démontre le théorème.

CONSÉQUENCE I. *Désignons par F_η l'ensemble de tous les points $p \subset M$ vérifiant la condition $\Phi(p) \geq \eta$. L'ensemble F_η étant un ensemble complémentaire à l'ensemble D_η du type G_δ il est un ensemble du type F_σ c'est-à-dire qu'il peut être représenté sous la forme*

$$F_\eta = \sum_{i=1}^{\infty} F_\eta{}^i \tag{1}$$

où $F_\eta{}^i$ est un ensemble formé.

CONSÉQUENCE II. *L'ensemble D_η et F_η sont des ensembles mesurables.*

Théorème II. *L'ensemble D de tous les points $p \subset M$ satisfaisant à la condition $\Phi(p) = 0$ est un ensemble du type G_δ.*

Donnons nous une suite de nombre positifs décroissants:

$$\eta_1, \eta_2, \cdots, \eta_n, \cdots$$

convergeant vers zéro.

Désignons par D_{η_k} l'ensemble de tous les points $p \subset M$ tels que $\Phi(p) < \eta_k$. Alors, il est évident que

$$D = \prod_{i=1}^{\infty} D_{\eta_i}.$$

Par conséquent, l'ensemble D étant la partie commune d'une suite dénombrable des ensembles du type G_δ, il est, lui-aussi, un ensemble du type G_δ.

Conséquence I. *Désignons par F l'ensemble de tous les points $p \subset M$ satisfaisant à la condition $\Phi(p) \neq 0$. L'ensemble F étant un ensemble complémentaire à l'ensemble D du type G_δ, il est un ensemble du type F_σ, c'est-à-dire qu'il peut être représenté sous la forme*

$$F = \sum_{i=1}^{\infty} F_i$$

où F_i est un ensemble formé.

Conséquence II. *Les ensembles D et F sont des ensembles mesurables.*

II.

5. Nous allons considérer maintenant les systèmes dynamiques dans lesquels tous les ensembles de mesure positive sont récurrent.

Préalablement démonstrons le lemme suivant:

Lemme I. *Soit $\mathfrak{M}$ un ensemble mesurable et admettons que, pour tout $p \subset \mathfrak{M}$ soit vérifiée la condition $\Phi(p) \neq 0$; si* mes $\mathfrak{M} > 0$, *il se trouvera un ensemble borné $\mathfrak{M}^* \subset \mathfrak{M}$,* mes $\mathfrak{M}^* > 0$ *qui est un ensemble errant.*

Nous nous bornerons à la démonstration du lemme pour le temps croissant; pour le temps décroissant le lemme est démontre d'une manière analogue.

Donnons nous une suite de nombres positifs

$$\eta_1, \eta_2, \cdots, \eta_n, \cdots$$

convergeant vers zéro.

Soit F un ensemble de tous les points $p \subset M$ pour lesquels $\Phi(p) = 0$ et F_{η_i} un ensemble de tous les points pour les quels $\Phi(p) \geq \eta_i$; alors

$$F = \sum_{i=1}^{\infty} F_{\eta_i}$$

Vu que $\mathfrak{M} \subset F$ et en posant $\mathfrak{M}_i = \mathfrak{M} \cdot F_{\eta_i}$ nous pouvons écrire

$$\mathfrak{M} = \sum_{i=1}^{\infty} \mathfrak{M}_i. \tag{3}$$

Chacun de ces ensembles est un ensemble mesurable, car il est la partie commune d'un ensemble mesurable et d'un ensemble du type F_σ. Mais on a $\operatorname{mes} \mathfrak{M} > 0$, donc, en vertu (3), il se trouvera un ensemble $\mathfrak{M}_k$ tel que $\operatorname{mes} \mathfrak{M}_k > 0$. Choisissons, dans l'espace M, un domaine Γ au diamètre $d < \eta_k$, et tel que, pour l'ensemble $\mathfrak{M}'_k = \mathfrak{M}_k \cdot \Gamma$, on ait $\operatorname{mes} \mathfrak{M}'_k > 0$.

Soit

$$\tau_1, \tau_2, \cdots, \tau_n, \cdots$$

une suite de nombres positifs croissant. Désignons par $\mathfrak{M}_k{}^m$ l'ensemble de points $p \subset \mathfrak{M}'_k$ pour lesquels soit vérifiée la condition $f(p, t) \not\subset \Gamma$ pour tout $t \geq \tau_m$. Il est évident que

$$\mathfrak{M}'_k = \sum_{m=1}^{\infty} \mathfrak{M}_k{}^m. \tag{4}$$

Montrons que, pour tout m, l'ensemble $\mathfrak{M}_k{}^m$ est fermé par rapport à $\mathfrak{M}'_k$, et que, par conséquent, c'est un ensemble mesurable.

Soit $q \subset \mathfrak{M}'_k$ un point limite pour $\mathfrak{M}_k{}^m$ et supposons que $q \not\subset \mathfrak{M}_k{}^m$. Alors, il se trouvera un $t_1 > \tau_m$ tel que $f(q, t_1) \subset \Gamma$. Choisissons un nombre $\epsilon > 0$ assez petit pour qu'on ait $S(q, \epsilon) \subset \Gamma$ et $S(f(q, t), \epsilon) \subset \Gamma$.

Choisissons ensuite un nombre $\delta > 0$ assez petit pour qu'on ait

$$f(S(q, \delta), t) \subset S(f(q, t), \epsilon) \tag{5}$$

pour tout $|t| \leq t_1$. En vertu de la dépendance continue des trajectoires des données initiales, il est toujours possible de trouver un δ.

Le point q est un point limite pour $\mathfrak{M}_k{}^m$, donc, il se trouvera un point $p' \subset \mathfrak{M}_k{}^m$ tel que $p' \subset S(q, \delta)$. Mais alors, conformement à (5), nous aurons $f(p', t_1) \subset \Gamma$, ce qui est impossible.

Ainsi, tous les $\mathfrak{M}_k{}^m$ sont mesurables. Mais on a $\operatorname{mes} \mathfrak{M}'_k > 0$, et alors, en vertu de (4), il se trouvera un ensemble $\mathfrak{M}_k{}^\nu$ tel que $\operatorname{mes} \mathfrak{M}_k{}^\nu > 0$. De plus, l'ensemble $\mathfrak{M}_k{}^\nu$ est borné et l'on a $f(\mathfrak{M}_k{}^\nu, t) \cdot \mathfrak{M}_k{}^\nu = 0$ pour tout $t > \tau_\nu$. En posant $\mathfrak{M}^* = \mathfrak{M}_k{}^\nu$, nous terminons la démonstration de notre lemme.

THÉORÈME III. *Si dans l'espace M tout ensemble de mesure positive est récurrent, tous les points de M, sauf un ensemble de mesure nulle, sont situés sur les trajectoires des mouvements stables au sens de Poisson.*

Admettons que le théorème ne soit pas vrai et supposons que l'ensemble F de tous les points $p \subset M$ pour lesquels on a $\Phi(p) \neq 0$ est un ensemble de mesure positive. Alors, en vertu du Lemme 1 on peut trouver un ensemble errant de mesure positive contenu dans M ce qui est en contradiction avec la condition du théorème.

Poincaré a démontré, que si le système dynamique admet un invariant integral et l'espace sur lequel il est défini est de mesure finie, tout ensemble de mesure positive est récurrent. Par conséquent, à cette classe des systèmes dynamiques est applicable le théorème qui est démontré plus haut et ainsi on obtient le " Wiederkehrsatz " de Carathéodory.

6. Construisons un exemple de système dynamique, dans lequel tout ensemble de mesure positive est récurrant et dans le quel, toutefois, aucun invariant integral ne peut être introduit.

Préalablement définissons une certaine fonction auxiliaire $\eta = g(\xi)$. A cet effet, introduisons sur le plan Euclidien E^2 un système de coordonnées cartésiennes orthoganales, et construisons sur les axes des coordonnées, les segments $-\frac{1}{2} \leq \xi \leq +\frac{1}{2}$ et $-\frac{1}{2} \leq \eta \leq +\frac{1}{2}$.

Considérons deux suites de nombres

$$\alpha_n = \frac{1}{3^n}, \qquad \beta_n = \frac{1}{4^n} \qquad\qquad (n = 1, 2, \cdots).$$

Prenons, sur l'axe ξ l'intervalle ouvert Δ_1 de longueur α_1 dont le centre soit l'origine des coordonnées et, sur l'axe η un intervalle ouvert d_1 le longueur β_1, dont le centre coïncide également avec l'origine des coordonnées. Sur l'intervalle Δ_1, soit $g(\xi)$ la fonction linéaire croissante dont les valeurs, sur Δ_1, forment l'intervalle d_1 sur l'axe η. Sur les deux segments complémentaires à l'intervalle Δ_1, construisons les intervalles ouverts Δ_2^1 et Δ_2^2 (les indices supérieurs croissent dans les sens positif de l'axe des abscisses) chacun de longueur α_2 et disposés de manière que leur centre coïncide avec les centres des segment qui les contiennent. Sur les intervalles Δ_2^1 et Δ_2^2, soit $g(\xi)$ la fonction linéaire croissante dont les valeurs sur les intervalles Δ_2^1 et Δ_2^2, forment respectivement les intervalles ouverts d_2^1 et d_2^2 sur l'axe η, chacun de la longuer β_2 et tels que leurs centres coinçident avec les centres des deux intervalles complementaires à d_1 (les indices supérieurs croissent dans les sens positif de l'axe des ordonnées).

Poursuivons ce procédé à l'infini.

Désignons par Γ et G les ensembles ouverts des points, appartenant à tous les intervalles construits respectivement sur les axes ξ et η.

La fonction $g(\xi)$ est définie sur l'ensemble Γ, l'ensemble G étant celui de ses valeurs; cette fonction est croissante et continue sur l'ensemble Γ.

Considérons les ensembles parfaits Π et P partout non denses qui sont complémentaires respectivement aux ensembles Γ et G. La fonction $g(\xi)$ n'étant pas encore définie dans les points $\xi \subset \Pi$, nous posons, dans ces points:

$$g(\xi) = \lim_{\substack{\xi' \to \xi \\ \xi' \subset \Gamma}} g(\xi')$$

Il est évident que cette limite existe.

La fonction est définie à présent, sur les segments $-\frac{1}{2} \leq \xi \leq +\frac{1}{2}$; il est aisé de voir que c'est une fonction croissante et continue; l'ensemble de ses valeurs est le segment $-\frac{1}{2} \leq \eta \leq +\frac{1}{2}$.

Ainsi la fonction $g(\xi)$ détermine la représentation binnivoque et continue du segment $-\frac{1}{2} \leq \xi \leq +\frac{1}{2}$ sur le segment $-\frac{1}{2} \leq \eta \leq +\frac{1}{2}$ avec lequel l'ensemble Π devient l'ensemble P.

Il est aisé de montrer qu'on a

$$\text{mes}\,\Pi = 0, \qquad \text{mes}\,P = \tfrac{1}{2}.$$

Reprenons maintenant le plan, euclidien E^2 et introduisons les coordonnées cartésiennes orthoganales x, y. Considérons l'ensemble L définie par les inégalités

$$-\tfrac{1}{2} \leq y \leq +\tfrac{1}{2}.$$

Recouvrons l'ensemble L par une famille de lignes brisées $y = F(x, C)$ qui dépendent d'un paramètre C, avec $-\frac{1}{2} \leq C \leq +\frac{1}{2}$ la fonction $F(x, C)$ étant une fonction périodique de la période 2π. Sur le segment $-\pi \leq x \leq +\pi$, nous définissons la fonction $F(x, C)$ de la manière suivante:

$$F(x, C) = \begin{cases} C, si -\pi \leq x \leq -\frac{3}{2} \\ [g(C) - C]x + [\frac{3}{2}g(C) - \frac{1}{2}C] si -\frac{3}{2} \leq x \leq -\frac{1}{2} \\ g(C), si -\frac{1}{2} \leq x \leq +\frac{1}{2} \\ [C - g(C)]x + [\frac{3}{2}g(C) - \frac{1}{2}C] si +\frac{1}{2} \leq x \leq +\frac{3}{2} \\ C\, si +\frac{3}{2} \leq x \leq +\pi \end{cases}$$

où $g(C)$ est la fonction définie plus haut.

Le fait que la fonction $g(C)$ est croissante et continue, il resulte que, par chaque point de l'ensemble L, il ne passe qu'une courbe et que deux courbes peuvent être aussi rapprochées qu'on veut si elles passent par deux points suffisemment repprochés.

Nous pouvons remplacer la famille des lignes brisées que nous venons de construire par une famille de lignes courbes aux dérivées continues, qui leur sont très rapprochées. Ceci peut-être éffectué de la manière suivante.

Soit $\delta > 0$, mais très petit et dans tous les cas inférieur à $\frac{1}{4}$. Alors, la famille des courbes $y = U(x, C)$ ou

$$U(x, C) = \frac{1}{2\delta} \int_{x-\delta}^{x+\delta} F(\alpha, C) d\alpha$$

aura les propriétés voulues.

Passons à présent à la construction de l'exemple d'un système dynamique.

Prenons un espace euclidien à trois dimensions E^3, introduisons-y un système de coordonnées cylindrique r, ϕ, z et considérons la surface cylindrique T définie par les conditions

$$r = 1, \qquad -\tfrac{1}{2} \leq z \leq +\tfrac{1}{2}.$$

Considérons ensuite sur la surface de T la famille des courbes:

$$z = U(\phi, C) = \frac{1}{2\delta} \int_{\phi-\delta}^{\phi+\delta} F(\alpha, C) d\alpha$$

chacune de ces courbes est fermée.

Finissons à présent sur la surface de T le système dynamique de manière que ses mouvements satisfassent aux équations

$$\frac{d\phi}{dt} = 1$$
$$z = U(\phi, C).$$

Tous les mouvements de ce système sont des mouvements périodiques, par suite tout sous-ensemble non vide T est un ensemble récurrent.

Montrons maintenant que ce système dynamique n'admet pas d'invariants intégraux.

Prenons sur la surface de T un segment de la droite $\phi = 0$ construisons-y l'ensemble P et considerons l'ensemble P^* de tous les points de T dont les coordonnées satisfont à l'inégalité $-\frac{1}{4} \leq \phi \leq +\frac{1}{4}$ et qui sont situés sur les trajectoires ayant des parties communes avec P. En même temps considérons sur T un segment de la droite $\phi = \pi$, construisons-y l'ensemble Π et considérons l'ensemble Π^* de tous les points de T dont les coordonnées satisfont aux l'inégalités $\pi - \frac{1}{4} \leq \phi \leq \pi + \frac{1}{4}$ et qui sont situés sur les trajectoires ayant des parties communes avec Π.

Il est aisé de voir, que

$$\text{mes } P^* = \tfrac{1}{4}, \qquad \text{mes } \Pi^* = 0$$

et que

$$f(P^*, \pi) = \Pi^*.$$

Nous voyons que l'ensemble P^* de mesure positive correspond à l'ensemble Π^* de mesure nulle, donc le système dynamique n'admet pas d'invariants intégraux.

III.

7. Démontrons maintenant un théorème de caractère descriptif dual au Théorème III complétant les resultats obtenus plus haut. Ce théorème est applicable à une classe plus large de mouvements dynamique que le Théorème III.

Préalablement démontrons le lemme suivant.

LEMME II. *Admettons que, pour tous les points p d'un ensemble $G \subset M$ est vérifiée la condition $\Phi(p) \neq 0$; si G est un ensemble de la seconde catégorie de R. Baire, il se trouvera dans M un ensemble ouvert G^*, qui est errant.*

Nous nous bornerons à la démonstration de lemme pour le temps croissant; pour le temps décroissant le lemme se démontre d'une manière analogue.

Soit

$$\eta_1, \eta_2, \cdots, \eta_n, \cdots$$

une suite de nombres positifs convergeante vers zéro et telle que $\eta_k > \eta_{k+1}$. Soit F_{η_k} l'ensemble de tous les points pour lesquels $\Phi(p) \geq \eta_k$; alors

$$F = \sum_{i=1}^{\infty} F_{\eta_i}$$

En posant $G_i = G \cdot F_{\eta_i}$ et on observant que $G \subset F$ nous pouvons écrire

$$G = \sum_{i=1}^{\infty} G_i\,. \tag{6}$$

L'ensemble G est un ensemble de la seconde catégorie de R. Baire, donc en vertu de (6) un des ensemble G_k est seconde catégorie.

Recouvrons l'ensemble G_k par une infinité dénombrable d'ensembles ouverts, dont les diamètres ne surpassent pas η_k; alors on peut indiquer un domaine Γ tel que l'ensemble $G'_k = G_k \cdot \Gamma$ est de seconde catégorie.

Soit

$$\tau_1, \tau_2, \cdots, \tau_n, \cdots$$

une suite de nombres positifs croissant. Désignons par $G_k{}^m$ l'ensemble de points $p \subset G'_k$ pour lesquels est vérifiée la condition $f(p, t) \not\subset \Gamma$ pour tout $t \geq \tau_m$.

Il est évident que

$$G'_k = \sum_{m=1}^{\infty} G_k{}^m \tag{7}$$

mais l'ensemble G'_k est un ensemble de la seconde catégorie de R. Baire et par suite en vertu de (7) on peut indiquer un ensemble G_k^{ν} qui n'est pas dense nulle part.

Soit $G^* \subset \Gamma$ un ensemble ouvert dans lequel l'ensemble de points appartenant à G_k^{ν} est dense partout. Montrons à présent que $f(G^*, t) \cdot G^* = 0$ pour tout $t \geq \tau_\nu$, Admettons le contraire; il se trouverait alors un point $q \subset G^*$ et un nombre $t_1 \geq \tau_\nu$ tels que $f(q, t_1) \subset G^*$. Soit $\epsilon > 0$ suffisemment petit pour que $S(q, \epsilon) \subset G^*$ et $S(f(q, t_1), \epsilon) \subset G^*$. Choissons ensuite un nombre $\delta > 0$ assez petit pour que

(8) $$f(S(q, \delta), t) \subset S(f(q, t), \epsilon) \cdots$$

pour tout $|t| \leq t_1$.

L'ensemble G_k^{ν} est partout dense dans G^*, donc, il se trouvera un point $p' \subset G_k^{\nu}$ tel que $p' \subset S(q, \delta)$. Mais alors, conformément à (8) nous aurons $f(p', t_1) \subset S(f(q, t_1), \epsilon) \subset G^* \subset \Gamma$, ce qui est impossible. Le lemme est démontré.

Dans ses recherches bien connues sur la théorie générale des systèmes dynamique G. D. Birkhoff a montré, que si dans l'espace sur lequel le système dynamique est défini tout ensemble ouvert est récurrent—l'ensemble de points situés sur les trajectoires stables au sens de Poisson est partout dense.

En s'appliquant sur notre lemme, on peut démontrer un énoncé plus précis, que celui de G. D. Birkhoff, à savoir:

THÉORÈME IV. *Si dans l'espace M tout ensemble ouvert est récurrent, tous les points de M, sauf un ensemble de la première catégorie de R. Baire, sont situés sur les trajectoires des mouvements stables au sens de Poisson.*

Admettons que le théorème ne soit pas vrai, et soit F l'ensemble de tous les points $p \subset M$ pour lesquels est vérifiée la condition $\Phi(p) \neq 0$; F est un ensemble de la second catégorie de R. Baire. Alors, en vertu du Lemme II on trouverait un ensemble ouvert G^* qui est errant. Mais ceci contredit la condition du théorème.

8. En terminant citons l'exemple d'un système dynamique dans lequel tout domaine est récurrent et dans lequel, toutefois il y a des ensembles errants de mesure positive.

Considérons, sur l'axe des abscisses un segment de la longueur 1 avec les coordonnées des extrémités $-\frac{1}{2}$ et $+\frac{1}{2}$ et construisons-y l'ensemble suivant P fermé, partout non dense.

Prenons une suite de nombres

$$\alpha_n = \frac{1}{4^n}, \qquad (n = 1, 2, \cdots).$$

Sur le segment $-\frac{1}{2} \leq x \leq +\frac{1}{2}$ prenons un intervalle de longueur α_1, de manière que son centre coïncide avec le centre du segment primitif. Sur chacun des deux segments complémentaires à l'intervalle qui vient d'être construit, prenons un intervalle de longueur α_2, les centres de ces intervalles coïncidant avec le centre des segments qui les contiennent. Poursuivons ce procédé indéfiniment et désignons par G l'ensemble des points qui appartiennent à tous les intervalles construits et par P l'ensemble compémentane sur le segment $-\frac{1}{2} \leq x \leq +\frac{1}{2}$.

Il est évident que l'ensemble P est un ensemble fermé partout non dense et que l'ensemble G est dense partout sur le segment primitif.

Au moyen de simples calculs on obtient

$$\text{mes } G = \tfrac{1}{2}, \qquad \text{mes } P = \tfrac{1}{2}.$$

L'ensemble de tous les intervalles que nous venons de construire est un ensemble dénombrable; soit

$$\Delta_1, \Delta_2, \cdots, \Delta_n, \cdots$$

la suite de ces intervalles. Désignons par a_n et par b_n les coordonnées d'extrémité droite et d'extrémité gauche de l'intervalle Δ_n. Définissons sur le segment $-\frac{1}{2} \leq x \leq +\frac{1}{2}$, la fonction $V(x)$ comme il suit:

$$V(x) = \begin{cases} 0 & \text{si } x \subset P \\ x - a_n & \text{si } a_n \leq x \leq a_n + \dfrac{b_n - a_n}{2} \\ b_n - x & \text{si } a_n + \dfrac{b_n - a_n}{2} \leq x \leq b_n. \end{cases}$$

La fonction $V(x)$ est évidemment continue sur le segment $-\frac{1}{2} \leq x \leq +\frac{1}{2}$. De plus, des simples calculs montrent que, pour deux points quelconques x_1 et x_2 du segment $-\frac{1}{2} \leq x \leq +\frac{1}{2}$ l'inégalité

$$| V(x_1) - V(x_2) | \leq | x_1 - x_2 |$$

est vérifiée; c'est à dire que la fonction $V(x)$ satisfait à la condition de Lipschitz.

Sur le plan euclidien E^2 où les coordonnées cartésiennes orthogonales x, y sont introduites considérons l'ensemble K de points (x, y) satisfaisant à la condition

$$x^2 + y^2 \leq (\tfrac{1}{2})^2.$$

Sur le diamètre de la circonférence K disposé sur l'axe x construisons un ensemble P et définissons sur K un système dynamique dont les équations différentielles sont

$$\frac{dx}{dt} = + y\{y^2 + V(x)\}$$
$$\frac{dy}{dt} = - x\{y^2 + V(x)\}.$$

De l'équation de la fonction $V(x)$ et de la forme des seconds membres de ces équations différentielles, il s'ensuit que ces membres sont des fonctions continues satisfaisant aux conditions de Lipschitz.

Il est aisé de voir que les courbes sur lesquelles se disposent les trajectoires de notre système dynamique forment une famille de circonférences concentriques dont le centre est à l'origine des coordonnées.

Quant au caractère des trajectoires mêmes, il est le suivant.

Tous les points appartenant à l'ensemble P construit sur l'axe des abscisses sont des points de repos, vu que dans ces points les seconds membres des équations différentielles s'annullent. En outre, l'origine des coordonnées est un points de repos. Les circonférences qui n'ont pas de parties communes avec l'ensemble sont des trajectoires des mouvements périodiques. L'ensemble des points situés sur ces circonférences est partout dense dans K, d'où il s'ensuit immédiatement que tous les domaines dans K sont des domaines récurrents. Quant aux circonférences qui ont des parties communes avec l'ensemble P, elles contiennent les trajectoires de quatre mouvements différents; de deux points d'équilibre sur l'axe x et de deux trajectoires de mouvements instables au sens de Poisson à savoir de circonférences ayant perdu les extrémités des arcs continus, aux points d'équilibre. Ces points d'équilibre sont les points limites alphe et oméga de deux mouvements instables au sens de Poisson.

Désignons par $\mathfrak{M}$ l'ensemble de points $p \subset K$ situés sur les trajectoires des mouvements instables au sens de Poisson. Il est évident que $\Phi(p) \neq 0$, si $p \subset \mathfrak{M}$, et que mes $\mathfrak{M} > 0$. Alors, en vertu du Lemme I, il se trouvera un ensemble $\mathfrak{M}^* \subset \mathfrak{M} \subset K$ qui est errant et de mesure positive. Il est aisé de dégager de K un ensemble analogue à $\mathfrak{M}^*$.

Moscou, U. S. S. R.

A TAUBERIAN THEOREM CONNECTED WITH THE PROBLEM OF THREE BODIES.*

By R. P. Boas, Jr.[1]

In a classical memoir on the problem of three bodies, K. F. Sundman[2] had occasion to consider a function $U(x)$, of class C' for $0 < x < c$, satisfying

$$A + \int_0^x P(t)\,dt = \frac{2}{x}\int_0^x tU(t)\,dt, \tag{1}$$

where $A > 0$, $P(t) \geqq 0$, and

$$2xU(x) \geqq A \qquad (0 < x < c). \tag{2}$$

He wished to show that

$$2xU(x) \to A \qquad (x \to 0+); \tag{3}$$

this relation, of course, does not in general follow from (1) and (2), but Sundman observed that (3) is a consequence of (1), (2), and a suitable auxiliary restriction on $U'(x)$; the auxiliary relation which Sundman used is

$$|U'(x)| \leqq BU(x)^2 \left\{ \frac{2xU(x) - Kx}{A - Kx} \right\}^{\frac{1}{2}} \qquad (0 < x < c), \tag{4}$$

where B and K are positive constants. My attention was called to this result of Sundman's by Professor Aurel Wintner, who pointed out that it is of the same general character as the well known "O-theorems" of Hardy and Littlewood,[3] although antedating their work by several years. Professor Wintner suggested to me that Sundman's theorem should be obtained as a special case of some simpler and more transparent general theorem. In this note I derive Sundman's theorem from the following theorem.

Theorem 1. *Let $f(x)$ be of class C^2 on $(0, \infty)$; let $\omega(y)$ be a positive increasing function in $y > 0$. If*

---

* Received May 23, 1938.

[1] National Research Fellow.

[2] K. F. Sundman, "Recherches sur le problème des trois corps," *Acta Societatis Scientiarum Fennicae*, vol. 34 (1907), no. 6. See pp. 10-16.

[3] G. H. Hardy and J. E. Littlewood, "Contributions to the arithmetic theory of series," *Proceedings of the London Mathematical Society*, (2), vol. 11 (1912-13), pp. 411-478; 416-428.

(5) $$f(x) = o(x) \qquad (x \to 0+)$$
and
(6) $$|f''(x)| = \omega(|f'(x)|)O(x^{-1}) \qquad (x \to 0+),$$
then
(7) $$f'(x) = o(1) \qquad (x \to 0+).$$

If $\omega(y)$ is a bounded function, Theorem 1 is a special case of a theorem of Hardy and Littlewood.[4] It is an elementary Tauberian theorem, but of a distinctly non-linear character because of the rather peculiar condition (6).

To reduce Sundman's theorem to Theorem 1, we note that (4) implies[5]

(8) $$|U'(x)| \leq CU(x)^{5/2}x^{1/2} \qquad (0 < x < c).$$

We set $g(x) = \int_0^x tU(t)\,dt$. From (1) we have
(9) $$g(x) \sim \tfrac{1}{2}Ax \qquad (x \to 0+).$$
From (2),
(10) $$g'(x) \geqq C > 0.$$

Now, using (8) and (10) we have, for $0 < x < c$,

$$\begin{aligned}|g''(x)| = |xU'(x) + U(x)| &\leq x^{3/2}U(x)^{5/2} + U(x) \\ &= x^{-1}g'(x)^{5/2} + x^{-1}g'(x)^{5/2}g'(x)^{-3/2} \leq Cx^{-1}g'(x)^{5/2}.\end{aligned}$$

Since (3) is equivalent to

$$g'(x) - \tfrac{1}{2}A = o(1) \qquad (x \to 0+),$$

Theorem 1, applied to a function $f(x)$ which is, for all sufficiently small x, equal to $g(x) - \frac{1}{2}Ax$, gives the desired result.

It is interesting to observe that (2) is a redundant hypothesis, since we have used only the weaker relation (10), which is actually implied by (8). For, (8) gives us

$$|dU(t)^{-3/2}/dt| \leqq Ct^{\frac{1}{2}}, \qquad |U(t)^{-3/2}| \leqq Ct^{3/2}, \qquad tU(t) \geqq C > 0.$$

Proof of Theorem 1. Let $\epsilon > 0$ be arbitrary. Then by (6) and (5) we can find $x_1 > 0$ such that, for some constant α,

(11) $$|f''(x)| < \alpha x^{-1}\omega(|f'(x)|) \qquad (0 < x < x_1),$$

(12) $$|f(x)| < \tfrac{1}{2}\epsilon x \qquad (0 < x < x_1).$$

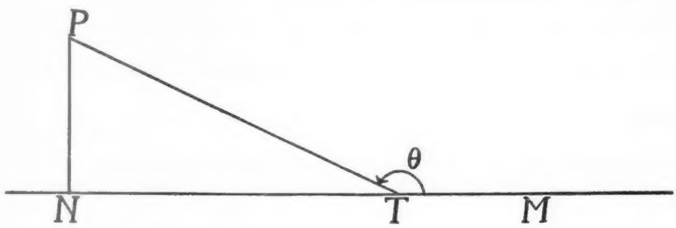
---

[4] G. H. Hardy and J. E. Littlewood, *op. cit.*, pp. 426-427.

[5] C is a generic notation for various positive constants.

We may assume without loss of generality that $\omega(0+) < 1$. The set E of points x such that $\omega(|f'(x)|) \leqq 1$ when $x \varepsilon E$ is not empty, and has $x = 0$ as a limit point. Otherwise we should have, for all sufficiently small x, either $f'(x) > \mu > 0$ or $f'(x) < -\mu < 0$, and consequently $f(x) = \left| \int_0^x f'(t)dt \right| > \mu x$, a contradiction of (5).

Consider the curve $\mathcal{C}$ whose equation is $y = f'(x)$; let P: (x_0, y_0) be a point of $\mathcal{C}$ such that $x_0 \varepsilon E$, $x_0 < \frac{1}{2}x_1$; we may suppose that $y_0 > 0$. Let N be the point $(x_0, 0)$; and M, the point $(2x_0, 0)$. Let T be a point on the x-axis such that $\tan\theta = -\alpha/x_0$, where θ is[6] the angle MTP.



For x between N and M, by (12),

$$|f(x)| < \tfrac{1}{2}\epsilon x \leqq \epsilon x_0. \tag{13}$$

Also, by (11),

$$\frac{dy}{dx} \geqq -|f''(x)| > -\alpha x^{-1}\omega(|y|) \geqq -\alpha x_0^{-1}\omega(|y|) = \omega(|y|)\tan\theta. \tag{14}$$

We now observe that when x is on the common part of NT and NM, $\mathcal{C}$ is above PT. This is evident for a point (x, y) of $\mathcal{C}$ for which $y \geqq y_0$. Since $\mathcal{C}$ passes through P, it cannot reach a point below PT until

$$\frac{dy}{dx} \leqq \tan\theta. \tag{15}$$

Since $\omega(y)$ is an increasing function, and $\omega(y_0) < 1$, (14) and (11) imply that (15) is impossible as long as $0 < y < y_0$; but since, for x between N and T, $\mathcal{C}$ cannot reach a point below the x-axis without crossing PT, we cannot have $y \leqq 0$ between N and T.

If T is to the left of M, $\mathcal{C}$ is above PT for x on NT, (13) holds, and consequently

---

[6] The figure is drawn for T to the left of M; but T may be on either side of M.

$$2\epsilon x_0 \geqq | f(x_1) - f(x_0) | = \left| \int_{x_0}^{x_1} y\, dx \right| \geqq \text{Area } PNT = -\tfrac{1}{2} y_0^2 \cot\theta,$$

so that

$$y_0 \leqq 2(\alpha\epsilon)^{1/2}. \tag{16}$$

If T is to the right of M, we have in the same way

$$2\epsilon x_0 \geqq \text{Area } PNM = \tfrac{1}{2} x_0 y_0, \qquad y_0 \leqq 2\epsilon^{1/2}. \tag{17}$$

Relations (16) and (17) show that $f'(x) \to 0$ as $x \to 0+$ in E. Therefore, because $f'(x)$ is continuous, for sufficiently small x_2 there are no points of the complement of E in $0 < x < x_2$; in fact, for x not in E, $| f'(x) | \geqq \mu > 0$, where $\omega(\mu) = 1$. This completes the proof.

The proof which we have given uses the method of Hardy and Littlewood; it can easily be adapted to prove the more general but less perspicuous

THEOREM 2. *Let $f(x)$ be of class C^2 on $(0, \infty)$; let $\omega(y)$ be a positive increasing function in $y > 0$; let $\phi(x)$ and $\psi(x)$ be positive functions in $x > 0$, such that, for some $r \geqq 0$, $x^{-r}\phi(x)$ and $x^{-r-2}\psi(x)$ are non-increasing, and*

$$\phi(x) = O(x^2\psi(x)), \qquad \phi(x)\psi(x) = O(1), \qquad (x \to 0).$$

If, as $x \to 0+$, $f(x) = o(\phi(x))$ and $f''(x) = \omega(| f'(x) |)O(\psi(x))$, then $f'(x) = o(\sqrt{[\phi(x)\psi(x)]})$.

If $\omega(y)$ is a constant, in which case the condition $\phi(x)\psi(x) = O(1)$ can be dropped, Theorem 2 reduces to one of the theorems of Hardy and Littlewood.[7]

PRINCETON UNIVERSITY.

[7] G. H. Hardy and J. E. Littlewood, *op. cit.*, pp. 426-427.

SOME EXTREMUM PROBLEMS IN THE THEORY OF FOURIER SERIES.*

By OTTO SZÁSZ.

1. Suppose $f(x)$ is a real- or complex-valued function, periodic of period 2π and Lebesgue integrable over $(-\pi, \pi)$. Denote its Fourier series by

$$(1) \qquad f(x) \sim \sum_{-\infty}^{\infty} c_\nu e^{i\nu x},$$

so that

$$(2) \quad c_\nu = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x) e^{-i\nu x} dx = \tfrac{1}{2}(a_\nu - ib_\nu), \qquad (\nu = 0, \pm 1, \pm 2, \cdots);$$

we assume throughout

$$(3) \qquad |f(x)| \leqq 1 \quad \text{for} \quad -\pi < x < \pi.$$

Let there be given $m + 1$ arbitrary real or complex numbers: $\mu_0, \mu_1, \cdots, \mu_m$, and an integer k. In § 2 we determine the maximum M_m of $|\sum_{\nu=0}^{m} \mu_\nu c_{\nu+k}|$ under the assumption (3) and the corresponding extremal functions $f(x)$. In § 3 we consider the extrema of $\Re \sum_0^{2n} \mu_\nu c_{\nu+k}$ and of $\Im \sum_0^{2n} \mu_\nu c_{\nu+k}$ in the subclass of real-valued functions $f(x)$ satisfying (3), and restricting the numbers μ_ν in a certain way. In § 4 the result is applied to sine series with positive coefficients, giving estimates for $\sum_1^n \nu b_\nu$ and for the partial sums. This is an improvement on the estimates, given previously [cf. 4, 5].[1] The results are extended in §§ 5 and 6 to generalised Fourier series of almost periodic functions and to Fourier integrals, improving on a result due to T. Takahashi [7], and sharpening previous estimates [3, 4, 5].

2. We have, using (2),

$$L_m \equiv \sum_0^m \mu_\nu c_{\nu+k} = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x) \sum_0^m \mu_\nu e^{-i(\nu+k)x} dx,$$

hence, by (3)

$$(4) \qquad |L_m| \leqq \frac{1}{2\pi}\int_{-\pi}^{\pi} \left|\sum_0^m \mu_\nu e^{-i\nu x}\right| dx = M_m.$$

* Presented to the Society December 29, 1937. Received by the Editors January 17, 1938.

[1] See the list of references at the end of this paper.

Equality holds here if $|f(x)| \equiv 1$ and if

$$f(x)e^{-ikx}\sum_0^m \mu_\nu e^{-i\nu x} \equiv \gamma \left| \sum_0^m \mu_\nu e^{-i\nu x} \right|, \text{ where } \gamma \text{ is a constant}$$

and $|\gamma| = 1$; this gives

$$(5) \qquad f(x) = \gamma e^{ikx} \left(\frac{\sum_0^m \bar{\mu}_\nu e^{i\nu x}}{\sum_0^m \mu_\nu e^{-i\nu x}} \right)^{1/2},$$

where $\bar{\mu}$ denotes the number conjugate to μ. If in particular m is even, $m = 2n$, and $\mu_0, \mu_1, \cdots, \mu_{2n}$ are defined by the identity

$$(6) \qquad \sum_0^{2n} \mu_\nu z^\nu \equiv \left(\sum_0^n \lambda_\nu z^\nu \right)^2,$$

that is

$$\mu_0 = \lambda_0^2,\ \mu_1 = 2\lambda_0\lambda_1, \cdots, \mu_n = \lambda_0\lambda_n + \lambda_1\lambda_{n-1} + \cdots + \lambda_n\lambda_0,$$
$$\mu_{n+1} = \lambda_1\lambda_n + \cdots + \lambda_n\lambda_1, \cdots, \mu_{2n} = \lambda_n^2,$$

then (4) gives

$$\left| \sum_{\nu=0}^{2n} \mu_\nu c_{\nu+k} \right| \leqq \sum_{\nu=0}^{n} |\lambda_\nu|^2, \qquad (k = 0, \pm 1, \pm 2, \cdots);$$

equality holds here if and only if

$$f(x) = e^{-i(\theta - kx)} \frac{\sum_0^n \bar{\lambda}_\nu e^{i\nu x}}{\sum_0^n \lambda_\nu e^{-i\nu x}}.$$

On replacing μ_ν by $\mu_\nu \xi^\nu$, where $|\xi| = 1$, (4) gives

$$(7) \qquad \boxed{\left| \sum_0^m \mu_\nu c_{\nu+k} \xi^\nu \right| \leqq \frac{1}{2\pi} \int_{-\pi}^{\pi} \left| \sum_0^m \mu_\nu e^{-i\nu x} \right| dx},$$

with equality sign, if

$$f(x) = e^{-i(\theta - kx)} \left(\frac{\sum_0^m \bar{\mu}_\nu e^{i\nu x} \xi^{-\nu}}{\sum_0^m \mu_\nu e^{-i\nu x} \xi^\nu} \right)^{1/2}.$$

For the case (6) we get

$$(8) \qquad \boxed{\left| \sum_0^{2n} \mu_\nu c_{\nu+k} \xi^\nu \right| \leqq \sum_0^n |\lambda_\nu|^2}.$$

where equality holds, if

$$f(x) = e^{i(kx-\theta)} \frac{\sum_0^n \bar{\lambda}_\nu \bar{\xi}^\nu e^{i\nu x}}{\sum_0^n \lambda_\nu \xi^\nu e^{-i\nu x}} = e^{-i\theta} e^{i(k+n)x} \xi^{-n} \frac{\sum_0^n \bar{\lambda}_\nu \bar{\xi}^\nu e^{i\nu x}}{\sum_0^n \lambda_\nu \xi^{\nu-n} e^{i(n-\nu)x}}.$$

Special cases:

a) $$\lambda_0 = 1, \lambda_1 = 1, \cdots, \lambda_n = 1.$$

We have from (8)

$$|c_k + 2c_{k+1}\xi + \cdots + (n+1)c_{k+n}\xi^n + nc_{k+n+1}\xi^{n+1} + \cdots + c_{k+2n}\xi^{2n}| \leqq n+1,$$

where equality holds, if

$$f(x) = e^{-i\theta} e^{i(k+n)x} \xi^{-n}.$$

The case $k = 1$ includes certain inequalities given by L. Fejér [1] and by M. Fekete [2].

b) $$\lambda_\nu = \binom{n}{\nu}, \qquad (\nu = 0, 1, \cdots, n).$$

Now $\mu_\nu = \binom{2n}{\nu}$, $\nu = 0, 1, \cdots, 2n$, and (8) gives

$$|\sum_0^{2n} \binom{2n}{\nu} c_{\nu+k} \xi^\nu| \leqq \sum_0^n \binom{n}{\nu}^2;$$

equality holds if

$$f(x) = e^{i(kx-\theta)} \left(\frac{1+\bar{\xi}e^{ix}}{1+\xi e^{-ix}}\right)^n = e^{i(kx-\theta)} e^{inx} \xi^{-n}.$$

In particular for $\xi = 1$

$$|\sum_0^{2n} \binom{2n}{\nu} c_{\nu+k}| \leqq \sum_0^n \binom{n}{\nu}^2,$$

with equality sign for $f(x) = e^{i(kx-\theta)} e^{inx}$.

c) $$\lambda_\nu = (-1)^\nu \binom{-\frac{1}{2}}{\nu}, \qquad (\nu = 0, 1, \cdots, n).$$

Now

$$\mu_\nu = 1, \qquad (\nu = 0, 1, \cdots, n)$$

$$\mu_\nu = (-1)^\nu \sum_{\rho=\nu-n}^n \binom{-\frac{1}{2}}{\rho}\binom{-\frac{1}{2}}{\nu-\rho} \equiv \gamma_\nu, \qquad (\nu = n+1, \cdots 2n).$$

$$|\sum_{\nu=0}^n c_{\nu+k}\xi^\nu + \sum_{n+1}^{2n} \gamma_\nu c_{\nu+k}\xi^\nu| \leqq 1 + \sum_1^n \left(\frac{1\cdot 3 \cdots (2\nu-1)}{2\cdot 4 \cdots 2\nu}\right)^2 \equiv G_n \sim \frac{1}{\pi}\log n.$$

3. We now assume $f(x)$ real valued, that is $c_{-\nu} = \bar{c}_\nu$. Then

$$(9) \qquad \sum_0^{2n} \mu_\nu c_{\nu+k} = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{-ikx} (\sum_0^n \lambda_\nu e^{-i\nu x})^2 f(x)\, dx$$
$$= \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{-i(k+n)x} (\sum_0^n \lambda_\nu e^{i(n/2-\nu)x})^2 f(x)\, dx.$$

Suppose

$$\lambda_\nu = \bar{\lambda}_{n-\nu}, \qquad (\nu = 0, 1, \cdots, n),$$

then

$$\sum_0^n \lambda_\nu e^{i(n/2-\nu)x} = \sum_0^n \bar{\lambda}_{n-\nu} e^{i(n/2-\nu)x} = \sum_0^n \bar{\lambda}_\nu e^{-i(n/2-\nu)x}.$$

Hence $\sum_0^n \lambda_\nu e^{i(n/2-\nu)x}$ is real, and (9) gives

$$\Re \sum_0^{2n} \mu_\nu c_{\nu+k} = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(x) \left(\sum_0^n \lambda_\nu e^{i(n/2-\nu)x} \right)^2 \cos (k+n)x \, dx$$

$$\Im \sum_0^{2n} \mu_\nu c_{\nu+k} = -\frac{1}{2\pi} \int_{-\pi}^{\pi} f(x) \left(\sum_0^n \lambda_\nu e^{i(n/2-\nu)x} \right)^2 \sin (k+n)x \, dx.$$

This yields

$$(10) \qquad \begin{aligned} \left| \Re \sum_0^{2n} \mu_\nu c_{\nu+k} \right| &\leqq \frac{1}{2\pi} \int_{-\pi}^{\pi} |\cos(k+n)x| \left(\sum_0^{2n} \mu_\nu e^{i(n-\nu)x} \right) dx \\ \left| \Im \sum_0^{2n} \mu_\nu c_{\nu+k} \right| &\leqq \frac{1}{2\pi} \int_{-\pi}^{\pi} |\sin(k+n)x| \left(\sum_0^{2n} \mu_\nu e^{i(n-\nu)x} \right) dx. \end{aligned}$$

But (cf. 6, p. 36)

$$|\sin x| = \frac{2}{\pi} \left(1 - 2 \sum_{\nu=1}^{\infty} \frac{\cos 2\nu x}{4\nu^2 - 1} \right),$$

and replacing x by $\pi/2 + t$

$$|\cos t| = \frac{2}{\pi} \left\{ 1 - 2 \sum_{\nu=1}^{\infty} (-1)^\nu \frac{\cos 2\nu t}{4\nu^2 - 1} \right\};$$

hence

$$|\cos(k+n)x| = \frac{2}{\pi} \left\{ 1 - 2 \sum_{\nu=1}^{\infty} (-1)^\nu \frac{\cos 2\nu(k+n)x}{4\nu^2 - 1} \right\},$$

$$|\sin(k+n)x| = \frac{2}{\pi} \left\{ 1 - 2 \sum_{\nu=1}^{\infty} \frac{\cos 2\nu(k+n)x}{4\nu^2 - 1} \right\}.$$

Assuming

$$2(k+n) > n, \quad \text{or} \quad 2k > -n,$$

from (10) by termwise integration

$$(11) \qquad \left| \Re \sum_0^{2n} \mu_\nu c_{\nu+k} \right| \leqq \frac{2\mu_n}{\pi} = \frac{2}{\pi} \sum_0^n \lambda_\nu \lambda_{n-\nu} = \frac{2}{\pi} \sum_0^n |\lambda_\nu|^2$$

$$(12) \qquad \left| \Im \sum_0^{2n} \mu_\nu c_{\nu+k} \right| \leqq \frac{2\mu_n}{\pi} = \frac{2}{\pi} \sum_0^n |\lambda_\nu|^2.$$

Equality holds in (11) if

$$\pm f(x) = \operatorname{sgn} \cos (k+n)x,$$

and in (12) if

$$\pm f(x) = \operatorname{sgn} \sin (k+n)x.$$

The function $f(x+t)$ has the Fourier coefficients

$$c_\nu(t) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x+t)e^{-i\nu x}dx = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(x)e^{-i\nu(x-t)}dx = e^{i\nu t}c_\nu,$$

and we find

$$| \Re \sum_{0}^{2n} \mu_\nu c_{\nu+k} e^{i(\nu+k)t} | \leqq \frac{2}{\pi} \sum_{0}^{n} | \lambda_\nu |^2 \tag{13}$$

$$| \Im \sum_{0}^{2n} \mu_\nu c_{\nu+k} e^{i(\nu+k)t} | \leqq \frac{2}{\pi} \sum_{0}^{n} | \lambda_\nu |^2. \tag{14}$$

Equality holds in (13) for a given t if

$$\pm f(x+t) \equiv \operatorname{sgn} \cos (k+n)x,$$

and in (14), if

$$\pm f(x+t) \equiv \operatorname{sgn} \sin (k+n)x.$$

In particular for $\lambda_\nu = 1$, $\nu = 0, 1, \cdots, n$, and $k = 1$

$$\begin{aligned} | \Re(c_1 e^{it} + 2c_2 e^{2it} + \cdots + nc_n e^{int} + (n+1)c_{n+1}e^{i(n+1)t} \\ + nc_{n+2}e^{i(n+2)t} + \cdots c_{2n+1}e^{i(2n+1)t}) | \leqq \frac{2}{\pi}(n+1), \end{aligned} \tag{15}$$

$$\begin{aligned} | \Im(c_1 e^{it} + \cdots + (n+1)c_{n+1}e^{i(n+1)t} + nc_{n+2}e^{i(n+2)t} \\ + \cdots + c_{2n+1}e^{i(2n+1)t} | \leqq \frac{2}{\pi}(n+1). \end{aligned} \tag{16}$$

Replacing t by $-t$, adding and subtracting yields

$$| \sum_{1}^{n} \nu a_\nu \cos \nu t + \sum_{n+1}^{2n} (2n-\nu)a_\nu \cos \nu t | \leqq \frac{4}{\pi} n, \tag{17}$$

$$| \sum_{1}^{n} \nu a_\nu \sin \nu t + \sum_{n+1}^{2n} (2n-\nu)a_\nu \sin \nu t | \leqq \frac{4}{\pi} n, \tag{18}$$

$$\left| \sum_{n}^{1} \nu b_\nu \begin{Bmatrix} \cos \nu t \\ \sin \nu t \end{Bmatrix} + \sum_{n+1}^{2n} (2n-\nu) b_\nu \begin{Bmatrix} \cos \nu t \\ \sin \nu t \end{Bmatrix} \right| \leqq \frac{4}{\pi} n. \tag{19}$$

With the notations

$$s_n(x) = \frac{a_0}{2} + \sum_{1}^{n} (a_\nu \cos \nu x + b_\nu \sin \nu x) \equiv \sum_{0}^{n} u_\nu$$

$$\bar{s}_n(x) = \sum_{1}^{n} (b_\nu \cos \nu x - a_\nu \sin \nu x)$$

$$\sigma_n(x) = \frac{s_0 + \cdots + s_{n-1}}{n}, \qquad \bar{\sigma}_n(x) = \frac{\bar{s}_0 + \cdots + \bar{s}_{n-1}}{n},$$

we have

$$\begin{aligned} \sigma_{2n}(x) - \sigma_n(x) &= \frac{1}{2n} \{ \sum_{0}^{2n-1} (2n-\nu)u_\nu - 2\sum_{0}^{n-1} (n-\nu)u_\nu \} \\ &= \frac{1}{2n} \{ \sum_{1}^{n} \nu u_\nu + \sum_{n+1}^{2n} (2n-\nu)u_\nu \}. \end{aligned}$$

Hence (15) and (16) give

$$\boxed{\begin{aligned} &(15') \qquad | \sigma_{2n}(t) - \sigma_n(t) | \leqq \frac{2}{\pi} \\ &(16') \qquad | \bar{\sigma}_{2n}(t) - \bar{\sigma}_n(t) | \leqq \frac{2}{\pi} \end{aligned}}.$$

4. We now suppose in addition

$$b_\nu \geqq 0, \qquad (\nu = 1, 2, 3, \cdots);$$

then (19) with $t = 0$ yields

$$(20) \qquad \boxed{\sum_1^n \nu b_\nu \leqq \frac{4}{\pi} n}, \qquad \left(\frac{4}{\pi} = 1 \cdot 2732 \cdots\right).$$

This is sharper than the estimate contained in a previous result [4, § 4]. For $n = 1$ [cf. 5]

$$b_1 \leqq \frac{4}{\pi},$$

and equality holds only for $f(x) \equiv 1$, $0 < x < \pi$, $f(-x) = -f(x)$, hence

$$f(x) = \frac{4}{\pi}\left(\frac{\sin x}{1} + \frac{\sin 3x}{3} + \cdots\right).$$

For $n > 1$ the smallest constant β_n satisfying

$$(21) \qquad \sum_1^n \nu b_\nu \leqq \beta_n \cdot n$$

is not known; but the example

$$\frac{\pi - x}{2} = \sum_1^\infty \frac{\sin \nu x}{\nu}$$

together with (20) gives

$$(22) \qquad \frac{2}{\pi} \leqq \beta_n \leqq \frac{4}{\pi}.$$

Using the identity

$$U_n = \frac{1}{n} \sum_1^{n-1} U_\nu + \frac{1}{n} \sum_1^n \nu u_\nu, \qquad U_n = \sum_1^n u_\nu = \sum_1^n b_\nu \sin \nu x,$$

and Fejér's theorem: $| \sum_1^{n-1} U_\nu | \leqq n$, (21) and (22) yield

$$(23) \qquad \boxed{| \sum_1^n b_\nu \sin \nu x | \leqq 1 + \beta_n \leqq 1 + \frac{4}{\pi} = 2 \cdot 2732 \cdots}.$$

On the other hand

$$\frac{2}{\pi}\sum_{1}^{n}\frac{1}{\nu}\sin\nu\frac{\pi}{n+1}\uparrow\frac{2}{\pi}\int_{0}^{\pi}\frac{\sin x}{x}\,dx>1\cdot 17.$$

If we assume only

$$b_\nu \geqq 0, \qquad (\nu=1,2,\cdots,N),$$

then (19) can be applied only for $n \leqq \frac{1}{2}N$, and (20) and (23) remain valid for $n \leqq \frac{1}{2}N$.

5. Similar results hold for generalized Fourier series and for Fourier integrals.

Let $\psi(x)$ be a measurable real function of the real variable x, let $\psi(-x) = -\psi(x)$. Suppose that $|\psi(x)| \leqq 1$, and that

$$\lim_{x\to\infty}\frac{1}{x}\int_{0}^{x}\psi(t)\sin\lambda t\,dt=b(\lambda)\equiv M\{\psi(t)\sin\lambda t\}$$

exists for all $\lambda>0$. It is known [cf. 3, p. 321], that $b(\lambda)$ vanishes, except for an enumerable set of λ-values. Denoting in a certain order by $\lambda_1,\lambda_2,\cdots$ those λ for which $b(\lambda)\neq 0$, the series

$$\sum_{1}^{\infty} b_n\sin\lambda_n x\sim\psi(x),\quad\text{where}\quad b_n=2b(\lambda_n),$$

is called the Fourier expansion of $\psi(x)$. We denote by $\rho_1,\rho_2,\cdots$ a subsequence of (λ_n), consisting of linearly independent numbers, and by (γ_n) the subsequence of those λ_n, which can be represented in the form

$$\lambda_n=\sum_{\nu=1}^{h} r_\nu\rho_\nu,\quad\text{where}\quad r_\nu=r_\nu(n)\ \text{ rational},\quad h=h(n)\ \text{ integer.}$$

Let q be a positive integer, $Q'=q\,!$, $P=qQ=q\cdot q\,!$, and

$$T_q(x)=\Sigma k_n^{(q)}b_n\sin\lambda_n x,$$

where

$$k_n^{(q)}=\prod_{a=1}^{q}\left(1-\frac{|\nu_a|}{P}\right)\quad\text{whenever}\quad 0<\lambda_n=\frac{1}{Q}\sum_{a=1}^{q}\nu_a\rho_a,\ \ \nu_a\ \text{integer,}$$

$|\nu_a|<P$, and $k_n^{(q)}=0$ for all other λ_n. Then

$$T_q(x)=M\{\psi(t)\tfrac{1}{2}[K_q(t-x)-K_q(t+x)]\},$$

where

$$K_q(t)=\prod_{a=1}^{q}\frac{1}{P}\left(\frac{\sin\dfrac{P}{2}\rho_a\dfrac{t}{Q}}{\sin\dfrac{\rho_a}{2Q}}\right)^{2};$$

thus from $|\psi(t)| \leqq 1$ it follows

$$|T_q(t)| \leqq 1. \tag{24}$$

We also introduce the "polynomials"

$$\begin{aligned} S_\eta(x,q) &= \sum_{0<\lambda_n\leqq\eta} \left(1-\frac{\lambda_n}{\eta}\right) k_n{}^{(q)} b_n \sin\lambda_n x \\ &= \frac{1}{\pi}\int_0^\infty \{T_q(x+2t)+T_q(x-2t)\}\frac{\sin^2\eta t}{\eta t^2}\,dt, \end{aligned} \tag{25}$$

and the expression

$$\begin{aligned} B(\eta) &= \frac{4}{\pi}\int_0^\infty T_q(t)\sin 2\eta t\,\frac{\sin^2\eta t}{\eta t^2}\,dt \\ &= \frac{4}{\pi}\int_0^\infty \sum k_n{}^{(q)} b_n \sin\lambda_n t \sin 2\eta t\,\frac{\sin^2\eta t}{\eta t^2}\,dt \\ &= \frac{2}{\pi}\sum k_n{}^{(q)} b_n \int_0^\infty \{\cos(\lambda_n-2\eta)t-\cos(\lambda_n+2\eta)t\}\frac{\sin^2\eta t}{\eta t^2}\,dt. \end{aligned}$$

Using the formula

$$\frac{2}{\pi}\int_0^\infty \cos 2kt\,\frac{\sin^2\eta t}{\eta t^2}\,dt = \begin{cases} 1-|k|/\eta & \text{if } |k|<\eta \\ 0 & \text{if } |k|\geqq\eta, \end{cases}$$

we get

$$\begin{aligned} B(\eta) &= \sum_{|\lambda_n-2\eta|<2\eta}\left(1-\frac{|\lambda_n-2\eta|}{2\eta}\right)k_n{}^{(q)}b_n \\ &= \sum_{0<\lambda_n\leqq2\eta}\left(1-\frac{2\eta-\lambda_n}{2\eta}\right)k_n{}^{(q)}b_n + \sum_{2\eta<\lambda_n<4\eta}\left(1-\frac{\lambda_n-2\eta}{2\eta}\right)k_n{}^{(q)}b_n \\ &= \frac{1}{2\eta}\sum_{0<\lambda_n\leqq2\eta}\lambda_n k_n{}^{(q)}b_n + \sum_{2\eta<\lambda_n<4\eta}\left(2-\frac{\lambda_n}{2\eta}\right)k_n{}^{(q)}b_n. \end{aligned}$$

On the other hand, using (24)

$$\begin{aligned} |B(\eta)| &\leqq \frac{4}{\pi}\int_0^\infty |\sin 2\eta t|\,\frac{\sin^2\eta t}{\eta t^2}\,dt = \frac{4}{\pi}\int_0^\infty |\sin 2\tau|\,\frac{\sin^2\tau}{\tau^2}\,d\tau \\ &= \frac{2}{\pi}\int_0^\pi |\sin 2\tau|\,d\tau = \frac{4}{\pi}\ \text{[cf. 6, p. 31 for a more general formula].} \end{aligned}$$

Replacing 2η by η and dividing by 2 we get finally

$$\left|\frac{1}{2\eta}\sum_{0<\lambda_n\leqq\eta}\lambda_n k_n{}^{(q)}b_n + \sum_{\eta<\lambda_n\leqq2\eta}\left(1-\frac{\lambda_n}{2\eta}\right)k_n{}^{(q)}b_n\right| \leqq \frac{2}{\pi}. \tag{26}$$

We now suppose

$$b(\gamma_n)\geqq 0 \quad\text{for}\quad 0<\gamma_n<\Omega,\quad \Omega>0,$$

and choose $\eta<\frac{1}{2}\Omega$; then from (26)

(27) $$\sum_{0<\lambda_n\leqq\eta} \lambda_n k_n{}^{(q)} b_n \leqq \frac{4}{\pi}\,\eta, \qquad 0<\eta<\tfrac{1}{2}\Omega.$$

Passing to the limit $q\to\infty$, we have $k_n{}^{(q)}\to 1$ if $\lambda_n\epsilon(\gamma_n)$, and (27) gives

(28) $$\boxed{\sum_{0<\gamma_n\leqq\eta} \gamma_n b(\gamma_n) \leqq \frac{2}{\pi}\,\eta},$$

which is analogous to the inequality (20).

Also from (25) and (24)

$$|\,S_\eta(x,q)\,| \leqq \frac{2}{\pi}\int_0^\infty \frac{\sin^2\eta t}{\eta t^2}\,dt = 1,$$

and from (27)

$$|\sum_{0<\lambda_n\leqq\eta} k_n{}^{(q)}\frac{\lambda_n}{\eta}\, b_n \sin\lambda_n x\,| \leqq \frac{4}{\pi};$$

combining these two inequalities:

$$|\sum_{\eta<\lambda_n\leqq 2\eta} k_n{}^{(q)} b_n \sin\lambda_n x\,| \leqq 1+\frac{4}{\pi}.$$

Writing $p_\nu{}^{(q)}$ for $k_n{}^{(q)}$ if $\lambda_n=\gamma_\nu$, we thus have

(29) $$|\,2\sum_{0<\gamma_\nu\leqq\eta} p_\nu{}^{(q)} b(\gamma_\nu)\sin\gamma_\nu x\,| \leqq 1+\frac{4}{\pi}.$$

It follows from (28) that $\sum_{0<\gamma_\nu\leqq\eta} b(\gamma_\nu)\sin\gamma_\nu x$ converges absolutely, hence passing to the limit $q\to\infty$ in (29), and writing $2\sum_{0<\gamma_\nu\leqq\eta} b(\gamma_\nu)\sin\gamma_\nu x=\psi_\eta(x)$,

$$\boxed{|\,\psi_\eta(x)\,| \leqq 1+\frac{4}{\pi}}, \qquad 0<\eta<\tfrac{1}{2}\Omega.$$

If (ρ_k) is a basic sequence of (λ_k), it follows that

$$\psi_\eta(x) = \sum_{0<\lambda_n\leqq\eta} b_n \sin\lambda_n x,$$

and this series converges absolutely. If in particular all $b_n>0$, then Ω and η are arbitrary. This result improves upon the one given in [4], § 6.

6. We now pass on to Fourier integrals. Let $g(x)$ belong to $L^p(0,\infty)$, $g(-x)=-g(x)$, and $|\,g(x)\,|\leqq 1$, $1<p\leqq 2$, $p'=p/(p-1)$. Then, as $a\to\infty$,

$$G(x,a) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\int_0^a g(t)\sin tx\,dt$$

converges in the mean with exponent p' [8, p. 96]

$$\lim_{a\to\infty}\int_0^\infty |\,G(x)-G(x,a)\,|^{p'}dx = 0.$$

$G(x)$ is the transform of $g(x)$, and we have

$$G(x)=\sqrt{\frac{2}{\pi}}\,\frac{d}{dx}\int_0^\infty g(t)\,\frac{1-\cos tx}{t}\,dt$$

$$g(x)=\sqrt{\frac{2}{\pi}}\,\frac{d}{dx}\int_0^\infty G(t)\,\frac{1-\cos tx}{t}\,dt$$

almost everywhere.

If $F(x)$ and $g(x)\in L^p(0,\infty)$, $1\leqq p\leqq 2$, and $f(x)$, $G(x)$ are their transforms, then [cf. 8, p. 54, 104]

$$\int_0^\infty F(x)G(x)\,dx=\int_0^\infty f(x)g(x)\,dx.$$

This gives in particular

$$S_\lambda(t)\equiv\int_0^\lambda\left(1-\frac{x}{\lambda}\right)G(x)\sin xt\,dx=\left(\frac{2}{\pi}\right)^{1/2}\frac{1}{\lambda}\int_{-\infty}^\infty g(x)\,\frac{\sin^2\frac{\lambda}{2}(t-x)}{(t-x)^2}\,dx.$$

We also consider

$$\begin{aligned}V_\lambda\equiv\int_0^\lambda\left(1-\frac{x}{\lambda}\right)G(x)\,dx&=\int_0^\lambda\left(1-\frac{x}{\lambda}\right)\left(\frac{2}{\pi}\right)^{1/2}\frac{d}{dx}\int_0^\infty g(t)\,\frac{1-\cos tx}{t}\,dt\,dx\\&=\left(\frac{2}{\pi}\right)^{1/2}\left(1-\frac{x}{\lambda}\right)\int_0^\infty g(t)\,\frac{1-\cos tx}{t}\,dt\Big]_{x=0}^{\lambda}\\&\quad+\left(\frac{2}{\pi}\right)^{1/2}\frac{1}{\lambda}\int_0^\lambda\int_0^\infty g(t)\,\frac{1-\cos tx}{t}\,dt\,dx\\&=\left(\frac{2}{\pi}\right)^{1/2}\frac{1}{\lambda}\int_0^\infty\frac{g(t)}{t}\int_0^\lambda(1-\cos tx)\,dx\,dt\\&=\left(\frac{2}{\pi}\right)^{1/2}\int_0^\infty g(t)\left(\frac{1}{t}-\frac{\sin\lambda t}{\lambda t^2}\right)dt.\end{aligned}$$

It follows from $|g(x)|\leqq 1$:

$$|S_\lambda(t)|\leqq\left(\frac{2}{\pi}\right)^{1/2}\int_{-\infty}^\infty\frac{\sin^2\frac{\lambda}{2}(t-x)}{\lambda(t-x)^2}\,dx=\left(\frac{2}{\pi}\right)^{1/2}\int_{-\infty}^\infty\frac{1}{2}\,\frac{\sin^2 u}{u^2}\,du=\left(\frac{2}{\pi}\right)^{1/2}\frac{\pi}{2}$$

or

$$|S_\lambda(t)|\leqq\left(\frac{\pi}{2}\right)^{1/2}. \tag{30}$$

Furthermore

$$\begin{aligned}|V_{2\lambda}-V_\lambda|&=\left(\frac{2}{\pi}\right)^{1/2}\left|\int_0^\infty g(t)\sin\lambda t\,\frac{1-\cos\lambda t}{\lambda t^2}\,dt\right|\\&\leqq\left(\frac{2}{\pi}\right)^{1/2}\cdot 2\int_0^\infty|\sin\lambda t|\,\frac{\sin^2\frac{\lambda}{2}t}{\lambda t^2}\,dt\\&=\left(\frac{2}{\pi}\right)^{1/2}\int_0^\infty\left(\frac{\sin t}{t}\right)^2|\sin 2t|\,dt=\frac{1}{\sqrt{2\pi}}\int_0^\pi|\sin 2t|\,dt=\left(\frac{2}{\pi}\right)^{1/2}.\end{aligned}$$

Or

$$\boxed{\left| \frac{1}{2\lambda}\int_0^\lambda xG(x)\,dx + \int_\lambda^{2\lambda}\left(1-\frac{x}{2\lambda}\right)G(x)\,dx \right| \leqq \left(\frac{2}{\pi}\right)^{\frac{1}{2}}}; \tag{31}$$

this is the inequality analogous to (26). We now suppose

$$G(x) \geqq 0, \qquad x > 0;$$

then from (31)

$$\boxed{\int_0^\lambda xG(x)\,dx \leqq 2\lambda\left(\frac{2}{\pi}\right)^{\frac{1}{2}}},$$

and

$$\left| \int_0^\lambda xG(x)\sin xt\,dx \right| \leqq 2\left(\frac{2}{\pi}\right)^{\frac{1}{2}}\lambda.$$

Combining this inequality with (30), finally

$$\boxed{\left| \int_0^\lambda G(x)\sin xt\,dx \right| \leqq 2\left(\frac{2}{\pi}\right)^{\frac{1}{2}} + \left(\frac{\pi}{2}\right)^{\frac{1}{2}}}. \tag{32}$$

As an analogue to a theorem of R. E. A. C. Paley on Fourier series T. Takahashi [7] proved (I quote from the *Zentralblatt für Mathematik*, vol. 15, p. 21): "let $f(x) \in L(0, \infty)$ and $|f(x)| \leqq M$, $x > 0$; let $F(x)$ be the cosine transform and $H(x)$ the sine transform of $f(x)$. If $F(x) \geqq 0$, $x > 0$, then

$$\left| \int_0^\omega F(u)\cos xu\,du \right| \leqq AM;$$

if $H(x) \geqq 0$, $x > 0$, then

$$\left| \int_0^\omega H(u)\sin xu\,du \right| \leqq BM\text{''};$$

A and B are universal constants. For cosine transforms we have given [5] the bound $\left(\frac{\pi}{2}\right)^{\frac{1}{2}}M$. This is the best possible, as is seen from the example:

$$f(x) = \left(\frac{2}{\pi}\right)^{\frac{1}{2}}\frac{\sin ax}{x}, \ |f(x)| \leqq a\left(\frac{2}{\pi}\right)^{\frac{1}{2}}, \ f(0) = a\left(\frac{2}{\pi}\right)^{\frac{1}{2}} = M, \ a > 0;$$

$$F(x) = \begin{cases} 1 \text{ for } 0 < x < a \\ 0 \text{ for } x > a. \end{cases}$$

$$\int_0^a F(u)\,du = a = \left(\frac{\pi}{2}\right)^{\frac{1}{2}}M.$$

For sine transforms we have given [2] [5] the bound

[2] There is a misprint in formulae (12) and (12′): replace $\left(\frac{\pi}{2}\right)^{-\frac{1}{2}}\pi^2$ by $\left(\frac{\pi}{2}\right)^{\frac{1}{2}}$.

$$M\left(\frac{\pi}{2}\right)^{1/2}\left[1+\frac{\alpha_0}{\sin^2\alpha_0}\right] < M\left(\frac{\pi}{2}\right)^{1/2}\times 2\cdot 38,$$

where α_0 is the root of a transcendental equation. (32) improves on this estimate, being

$$\frac{4}{\pi}=1\cdot 2732\cdots < \frac{\alpha_0}{\sin^2\alpha_0}=1\cdot 37\cdots.$$

To find a lower bound for the best possible choice of B let $g(x)=e^{-x}$, hence

$$G(x)=\left(\frac{2}{\pi}\right)^{1/2}\frac{x}{1+x^2} \quad [8, \text{ p. } 179].$$

Now

$$\int_0^\lambda \frac{x}{1+x^2}\sin x\frac{\pi}{\lambda}\,dx=\int_0^\lambda \frac{1}{x}\sin x\frac{\pi}{\lambda}\,dx-\int_0^\lambda \frac{1}{x}\,\frac{1}{1+x^2}\sin x\frac{\pi}{\lambda}\,dx$$
$$=\int_0^\pi \frac{\sin u}{u}\,du+O\left(\frac{1}{\lambda}\int_0^\lambda \frac{dx}{1+x^2}\right)\to\int_0^\pi\frac{\sin u}{u}\,du=1\cdot 8519\cdots$$

as $\lambda\to\infty$. Hence a lower bound for the best estimate in (32) is

$$\left(\frac{2}{\pi}\right)^{1/2}\int_0^\pi\frac{\sin u}{u}\,du.$$

The same bound is found by considering

$$g(x)=\frac{\sin x}{x},\qquad G(x)=\frac{1}{\sqrt{2\pi}}\log\left|\frac{1+x}{1-x}\right|,$$

and calculating

$$\frac{1}{\sqrt{2\pi}}\int_0^\lambda\log\left|\frac{1+x}{1-x}\right|\sin x\frac{\pi}{\lambda}\,dx$$

for large λ.

UNIVERSITY OF CINCINNATI.

REFERENCES.

1. L. Fejér, "On a theorem of Paley," *Bulletin of the American Mathematical Society*, vol. 40 (1934), pp. 469-475.
2. M. Fekete, "Proof of three propositions of Paley," *Ibid.*, vol. 41 (1935), pp. 138-144.
3. ———, "On generalized Fourier series with non-negative coefficients," *Proceedings of the London Mathematical Society*, ser. 2, vol. 39 (1935), pp. 321-333.
4. O. Szász, "On the partial sums of certain Fourier series," *American Journal of Mathematics*, vol. 59 (1937), pp. 696-708.

5. ———, "Fourier-sorok részletösszegeiröl (Über die Partialsummen Fourierscher Reihen)," Matematikai és Természettudományi Értesitö," vol. 56 (Budapest, 1937), pp. 382-396.
6. C. de la Vallée Poussin, *Leçons sur l'approximation des fonctions d'une variable réelle*, Paris, 1919.
7. T. Takahashi, "On positive Fourier transforms," *Science Reports Tôhoku University*, I. S., vol. 25 (1936), pp. 332-337.
8. E. C. Titchmarsh, *Introduction to the Theory of Fourier Integrals*, Oxford, 1937.

CORRECTIONS.

Corrections for a previous paper by the same author, *On the partial sums of certain Fourier series*, vol. 59 (1937), pp. 696-708.

P. 697, l. 3, read $(\pi - x)/2$ instead of $\pi - x/2$.

P. 697, l. 5, read $s_n[\pi/(n+1)]$ instead of $s_n(\pi/n+1)$.

P. 700, l. 5, read $x \to +0$ instead of $x \to \infty$.

P. 700, l. 6 from bottom, read Tables instead of Table

P. 701, formula (21), insert $a_0 +$, so as to read $a_0 + \sum_1^\infty \cdots$.

P. 701, last l. delete "in";

P. 705, l. 3, the formula on this line should be numbered (31).

P. 705, l. 3, replace ω by ψ.

P. 705, l. 6 from bottom, read $[K_q(t-x) - K_q(t+x)]$ instead of

$$[K_q(t-x) + K_q(t+x)].$$

P. 706, l. 1, read $\sum_{0<\lambda_n\leqq\mu}$ instead of $\sum_{0<\lambda_n\leqq\omega}$.

P. 706, l. 3, read $[T_q(x+2t) + T_q(x-2t)]$ instead of

$$[T_q(x+2t) - T_q(x-2t)].$$

P. 707, l. 1, read $0 < \omega \leqq \mu < \Omega$ instead of $0 < \omega < \Omega$.

P. 708, l. 10, read $a_0 + \sum_{0<\lambda_n\leqq\omega} (a_n \cos \lambda_n x + b_n \sin \lambda_n x)$ instead of

$$a_0 + \sum_{0<\lambda_n\leqq\omega} (a_n \cos nx + b_n \sin nx).$$

CORES OF COMPLEX SEQUENCES AND OF THEIR TRANSFORMS.*[1]

By Ralph Palmer Agnew.[2]

1. Introduction. Let $s_1, s_2, \cdots$ be a sequence of complex numbers. For each $n = 1, 2, 3, \cdots$, let C_n be the least convex closed set of the finite complex plane containing the points $s_n, s_{n+1}, \cdots$. Then obviously $C_1 \supset C_2 \supset \cdots$. Let $C = C_1 C_2 \cdots$ be the intersection of the sets $C_1, C_2, \cdots$. The set C (which is necessarily convex and closed) is called by Knopp[3] the *core* (Kern) of the sequence s_n. In case C contains just one point, s_n is convergent. In case C is empty (contains no finite point) the sequence s_n is called *definitely* (bestimmt) *divergent*, and we shall write $s_n \sim \infty$. For example, if s_n is n or in according as n is even or odd, then each set C_n consists of the part of the first quadrant of the complex plane remaining after removal of a triangular section with right angle at the origin; in this case it is easy to show that the core C of s_n is empty and hence that $s_n \sim \infty$. Likewise if $s_n = n + i(-1)^n n^2$, then $s_n \sim \infty$. If $s_n = ni^n$, then each C_n contains all points of the complex plane; hence C also contains all points of the complex plane and it is not true that $s_n \sim \infty$. If $s_n = (-1)^n$, then each C_n and hence C consists of the real axis and again $s_n \sim \infty$ fails.

A matrix $A \equiv \| a_{nk} \|$ of complex constants transforms a given sequence s_n into the sequence

$$A \qquad\qquad \sigma_n = \sum_{k=1}^{n} a_{nk} s_k,$$

and defines a method of summability A which assigns to the sequence s_n the value $\lim_{n \to \infty} \sigma_n$ when the limit exists. The method A is *regular* if it assigns to each convergent sequence the value to which it converges. If A is regular then the core Γ of the A transform σ_n of each convergent sequence s_n is identical with the core C of s_n, the two cores Γ and C each consisting of the single point which is the limit of the sequence s_n.

The well known Silverman-Toeplitz necessary and sufficient conditions for regularity of A are

* Received February 4, 1938.

[1] Presented to the American Mathematical Society, February 26, 1938.

[2] The author is indebted to Professor Otto Szász for a conversation which suggested the problem solved by Theorem 3.1, and to Professor W. A. Hurwitz for helpful criticisms.

[3] K. Knopp, "Zur Theorie der Limiterungsverfahren," *Mathematische Zeitschrift*, vol. 31 (1929-30), pp. 97-127, p. 115.

$$(1.1) \qquad \sum_{k=1}^{n} | a_{nk} | < M \qquad (n = 1, 2, \cdots)$$

$$(1.2) \qquad \lim_{n\to\infty} a_{nk} = 0 \qquad (k = 1, 2, \cdots)$$

$$(1.3) \qquad \lim_{n\to\infty} \sum_{k=1}^{n} a_{nk} = 1,$$

M being a constant.

Concerning real matrices a_{nk}, Knopp (*loc. cit.*, p. 115) has proved the Kernsatz. *If A is regular and*

$$(1.4) \qquad a_{nk} \geqq 0 \qquad (n, k = 1, 2, 3, \cdots)$$

then the core C of each sequence s_n contains the core Γ of its transform σ_n.

It follows, as Knopp points out (*loc. cit.*, p. 118), that if A is regular and satisfies (1.4), then $s_n \sim \infty$ implies $\sigma_n \sim \infty$.

In § 2 we give a characterization different from but equivalent to Knopp's definition of definite divergence. In § 3, we characterize the class of complex regular matrices A having the property that $s_n \sim \infty$ implies $\sigma_n \sim \infty$, and show that this class is identical with the class of complex regular matrices A having the property that $\mathfrak{R}(s_n) \to +\infty$ implies $\sigma_n \sim \infty$. In § 4, we show that a condition only slightly less restrictive than Knopp's condition (1.4) is necessary as well as sufficient to ensure that the core of each sequence s_n must contain the core of its transform σ_n. A corresponding theorem involving the class of bounded sequences is obtained.

In § 5 we give, with comments relevant to cores, a generalization of a theorem of Steinhaus [4] which can be phrased as follows:

Corresponding to each regular transformation A, there is a bounded sequence s_n such that the core of the transform σ_n contains more than one point.

We use $\mathfrak{R}(z)$ and $\mathfrak{I}(z)$ to denote the real and imaginary parts of z, so that $z = \mathfrak{R}(z) + i\mathfrak{I}(z)$.

2. A discussion of definitely divergent sequences. It is easy to show that if $s_n \sim \infty$, then $| s_n | \to \infty$. For if $s_n \sim \infty$, then C is empty. Since C is the intersection of the monotone decreasing sequence $C_1, C_2, C_3, \cdots$ of closed sets, it follows that corresponding to each $R > 0$ we can choose an index N such that C_N contains no point of the circle $| s | \leqq R$; then $| s_n | > R$ when $n \geqq N$ and $| s_n | \to \infty$. The example $s_n = (-1)^n n$ shows that $| s_n | \to \infty$ does not imply $s_n \sim \infty$. If the points s_n all lie in an angle $< \pi$ and $| s_n | \to \infty$,

[4] H. Steinhaus, "Some remarks on the generalizations of the notion of limit" (in Polish), *Prace mat. fiz.*, vol. 22 (1921), pp. 121-34.

then $s_n \sim \infty$. That the converse of the last statement does not hold follows from a consideration of the sequence $s_n = n + (-1)^n in^2$. A more significant theorem is the following.

THEOREM 2.1. *A necessary and sufficient condition that s_n be definitely divergent ($s_n \sim \infty$) is that an angle ϕ exist such that*

$$\lim_{n\to\infty} \mathcal{R}(s_n e^{i\phi}) = +\infty. \tag{2.11}$$

Sufficiency is easily established. If (2.11) holds, then for each $M > 0$ we can choose N such that $\mathcal{R}(s_n e^{i\phi}) > M$ when $n \geqq N$. It now becomes clear that the core of the sequence $s_n e^{i\phi}$ can contain no point with real part $< M$. Hence the core of $s_n e^{i\phi}$ is empty. Since the core of s_n is obtained by rotating the core of $s_n e^{i\phi}$, the core of s_n is empty, i. e. $s_n \sim \infty$.

To prove necessity, let $s_n \sim \infty$. With C_n defined as in § 1, there is a unique point P_n of C_n nearest the origin O, and if we put $P_n = \rho_n e^{i\phi_n}$ where $\rho_n \geqq 0$ and $-\pi < \phi_n \leqq \pi$, then $\lim_{n\to\infty} \rho_n = +\infty$. Choose N such that $\rho_n > 0$ when $n \geqq N$. When $n \geqq N$, the line L_n which is the perpendicular bisector of the line segment OP_n cannot intersect C_n, for otherwise convexity of C_n would imply that P_n is not the point of C_n nearest O. It follows that the point O and the set C_n lie on opposite sides of the line L_n. Consider first the case where $n > n' \geqq N$ exist such that $\phi_n \neq \phi_{n'}$. In this case the lines L_n and $L_{n'}$ divide the plane into four wedges, and the set C_n lies in the wedge W vertically opposite the wedge containing O. If we let ϕ be the angle through which the points of the plane must be rotated to bring the ray bisecting the wedge W into the direction of the positive real axis, we can show that $\lim_{n\to\infty} \mathcal{R}(s_n e^{i\phi}) = +\infty$. In the alternative case, $\phi_n = \phi_N$ for all $n \geqq N$. In this case, we can show that $\lim_{n\to\infty} \mathcal{R}(s_n e^{-i\phi_N}) = +\infty$ and Theorem 2.1 is proved.

We now give, for use later, a rather obvious lemma.

LEMMA 2.2. *If two sequences s_n and s'_n are so related that*

$$\lim_{n\to\infty} | s_n - s'_n | = 0, \tag{2.21}$$

then the cores C and C' of s_n and s'_n are identical.

To prove that $C' \subset C$, assume that z' is a point of C' not in C. Then there is an index p such that z' is not in C_p. Let z'' be the unique point of C_p nearest z'. Let $\alpha = z' + (z'' - z')/3$ and $\beta = z' + 2(z'' - z')/3$ and let $| z'' - z' | = 3d$ so that $| \alpha - z' | = | \beta - \alpha | = | z'' - \beta | = d$. Choose an index $q > p$ such that $| s_n - s'_n | < d$ when $n \geqq q$. Let L_α and L_β be the

lines perpendicular to the line $z'z''$ at α and β respectively. The points of C_p and hence the points $s_q, s_{q+1}, \cdots$ are all separated from z' by the line L_β, and it follows that the points $s'_q, s'_{q+1}, \cdots$ are all separated from z' by the line L_α. Therefore z' is not in C'_q and hence not in C'. This contradiction proves that $C' \subset C$. Likewise $C \subset C'$, and Lemma 2. 2 is proved.

3. Regular transformations. Considering regular matrices of complex elements a_{nk}, we prove

THEOREM 3. 1. *In order that a regular matrix A may have the property that $s_n \sim \infty$ implies $\sigma_n \sim \infty$, it is necessary and sufficient that an index K exist for which*

$$a_{nk} = \mathfrak{R}(a_{nk}) \geqq 0 \qquad k \geqq K. \tag{3.11}$$

The condition (3. 11) implies no restriction on the elements of the first $K-1$ columns of the matrix a_{nk}, but does imply that all elements in the K-th column and to the right of it are real and non-negative.

Proof of sufficiency for Theorem 3. 1 follows easily from the next lemma which is a trivial extension of Knopp's Kernsatz.

LEMMA 3. 2. *If A is regular and satisfies* (3. 11), *then the core C of each sequence s_n contains the core Γ of its transform.*

To prove this lemma, let A be regular, let (3. 11) hold, let s_n be a given sequence, and let $\sigma_n = \Sigma a_{nk}s_k$. If we set $a'_{nk} = 0$ or a_{nk} according as $k < K$ or $k \geqq K$, then the transformation

$$\sigma'_n = \sum_{k=1}^{n} a'_{nk}s_k$$

is regular and satisfies (1. 4). It follows from the Kernsatz that the core C of s_n contains the core Γ' of s'_n. But regularity of A implies that $\lim(\sigma'_n - \sigma_n) = 0$, and it follows that the core Γ of σ_n is the same as Γ'. Therefore $C \supset \Gamma$ and Lemma 3. 2 is proved.

As our first step in the proof of necessity for Theorem 3. 1, we establish

LEMMA 3. 3. *If A is regular and has the property that $s_n \sim \infty$ implies $\sigma_n \sim \infty$, then there is an index K_1 for which*

$$\mathfrak{J}(a_{nk}) \geqq 0 \qquad k \geqq K_1. \tag{3.31}$$

To prove this lemma, suppose A is regular and that (3. 31) fails. We construct a sequence $s_n = x_n + iy_n$ for which $x_n \to +\infty$ so that $s_n \sim \infty$ while $\sigma_n \sim \infty$ fails. To indicate the manner in which the elements of the sequence

s_n are determined, we assume that indices $1 = n_0 < \nu_1 < n_1 < \cdots < \nu_{p-1} < n_{p-1}$ have been defined, and assume that s_k has been defined for $1 \leqq k \leqq n_{p-1}$. Choose an index $\nu_p > n_{p-1}$ such that

$$\left| \sum_{k=1}^{n_{p-1}} a_{\nu_p k} s_k \right| < 1/2p$$

$$\left| 1 - \sum_{k=n_{p-1}+1}^{\nu_p} a_{\nu_p k} \right| < 1/2p \mid p + ip^2 \mid,$$

and let

$$s_k = p + ip^2 \qquad n_{p-1} < k \leqq \nu_p.$$

Then

$$\sigma_{\nu_p} = \sum_{k=1}^{n_{p-1}} a_{\nu_p k} s_k + (p + ip^2) \sum_{k=n_{p-1}+1}^{\nu_p} a_{\nu_p k}$$

so that

$$\begin{aligned} \mid \sigma_{\nu_p} - (p + ip^2) \mid &\leqq \left| \sum_{k=1}^{n_{p-1}} a_{\nu_p k} s_k \right| + \mid p + ip^2 \mid \; \left| 1 - \sum_{k=n_{p-1}+1}^{\nu_p} a_{\nu_p k} \right| \\ &< 1/2p + 1/2p = 1/p. \end{aligned}$$

Next, choose k_p and n_p such that $\nu_p < k_p \leqq n_p$ and $c < 0$ where

$$a_{n_p k_p} = b + ic.$$

Let

$$\begin{aligned} s_k &= p & \nu_p < k \leqq n_p,\ k \neq k_p \\ &= p + x + iy & k = k_p \end{aligned}$$

where x and y are real numbers to be determined presently. Setting

$$\alpha + i\beta = \sum_{k=1}^{\nu_p} a_{n_p k} s_k + \sum_{k=\nu_p+1}^{n_p} a_{n_p k} p,$$

we find

$$\begin{aligned} \sigma_{n_p} &= \alpha + i\beta + (b + ic)(x + iy) \\ &= (\alpha + bx - cy) + i(\beta + cx + by). \end{aligned}$$

Let V_p be the greatest real number such that $V_p \leqq -p$ and $cV_p - b\alpha - c\beta \geqq 0$. Let x and y be determined by the equation

$$\sigma_{n_p} \equiv (\alpha + bx - cy) + i(\beta + cx + by) = iV_p.$$

It turns out that $x \geqq 0$, and hence that $\mathfrak{R}(s_k) \geqq p$ when $k = k_p$.

The procedure outlined above furnishes a sequence

$$1 = n_0 < \nu_1 < n_1 < \nu_2 < n_2 < \cdots$$

of indices and a sequence s_k such that

$$\mathfrak{R}(s_k) \geqq p \qquad n_{p-1} < k \leqq n_p. \tag{3.32}$$

The transform σ_n of s_n is such that

$$\sigma_{\nu_p} = p + ip^2 + \epsilon_p; \qquad \sigma_{n_p} = iVp \qquad (p = 1, 2, \cdots) \tag{3.33}$$

where $\epsilon_p \to 0$ and $V_p \leqq -p$. The estimate (3. 32) implies that $s_n \sim \infty$. It follows from (3. 33), Lemma 2. 2, and the fact that the core of a sequence contains the core of each subsequence, that the core Γ of the sequence σ_n contains the core of the sequence τ_p defined by

$$\begin{aligned} \tau_p &= p + ip^2 & (p = 1, 3, 5, \cdots) \\ &= iV_p & (p = 2, 4, 6, \cdots). \end{aligned}$$

Since $|\tau_p| \to \infty$ and the sequence τ_p has an infinite set of points on the semi-parabola $z = x + ix^2$, $x \geqq 0$, and an infinite set on the negative imaginary axis, it can be shown that the core of τ_n is the closed right half-plane $\mathcal{R}(z) \geqq 0$. Hence the core Γ of σ_n contains this half-plane and $\sigma_n \sim \infty$ fails. This proves Lemma 3. 3.

If a matrix a_{nk} is regular and such that $s_n \sim \infty$ implies $\sigma_n \sim \infty$, the conjugate matrix $\bar{a}_{nk}$ also has these properties, and Lemma 3. 3 implies that there is an index $K_2 > K_1$ such that $\mathcal{J}(\bar{a}_{nk}) \geqq 0$ when $k \geqq K_2$, i. e. $\mathcal{J}(a_{nk}) \leqq 0$ when $k \geqq K_2$. Combining this result with Lemma 3. 3, we have

LEMMA 3. 4. *If A is regular and has the property that $s_n \sim \infty$ implies $\sigma_n \sim \infty$, then there is an index K_2 for which*

$$\mathcal{J}(a_{nk}) = 0 \qquad k \geqq K_2. \tag{3.41}$$

We complete the proof of Theorem 3. 1 by proving

LEMMA 3. 5. *If A is regular and satisfies* (3. 41) *but not* (3. 11), *then there exists a real sequence s_n of non-negative real elements for which $s_n \to +\infty$ while the core Γ of the transform σ_n is the entire real axis.*

Choose K_2 such that (3. 41) holds and let $s_k = 0$ when $1 \leqq k < K_2$. Suppose now that indices $K_2 = n_0 < \nu_1 < n_1 < \cdots < \nu_{p-1} < n_{p-1}$ have been defined, and that s_k has been defined for $1 \leqq k \leqq n_{p-1}$. Choose $\nu_p > n_{p-1}$ such that

$$\Big|\sum_{k=1}^{n_{p-1}} a_{\nu_p k} s_k\Big| < 1/2p; \qquad \Big|1 - \sum_{k=n_{p-1}+1}^{\nu_p} a_{\nu_p k}\Big| < 1/2p^2$$

and put

$$s_k = p \qquad n_{p-1} < k \leqq \nu_p.$$

Then

$$\sigma_{\nu_p} = \sum_{k=1}^{n_{p-1}} a_{\nu_p k} s_k + p \sum_{k=n_{p-1}+1}^{\nu_p} a_{\nu_p k}$$

so that

$$|\sigma_{\nu_p} - p| \leqq \Big|\sum_{k=1}^{n_{p-1}} a_{\nu_p k} s_k\Big| + p\Big|1 - \sum_{k=n_{p-1}+1}^{\nu_p} a_{\nu_p k}\Big| < 1/2p + 1/2p = 1/p.$$

Next, choose k_p and n_p such that $\nu_p < k_p \leqq n_p$ and $a_{nk} < 0$ when $n = n_p$, $k = k_p$. Let

$$\begin{aligned} s_k &= p & \nu_p < k \leqq n_p,\ k \neq k_p \\ &= p + x & k = k_p \end{aligned}$$

where x is chosen such that $x \geqq 0$ and

$$\sigma_{n_p} = \sum_{k=1}^{\nu_p} a_{n_pk}s_k + p \sum_{k=\nu_p+1}^{n_p} a_{n_pk} + a_{n_pk_p}x < -p.$$

This procedure furnishes indices $K_2 = n_0 < \nu_1 < n_1 < \nu_2 < n_2 \cdots$ and a sequence s_n of real non-negative elements for which

$$s_k \geqq p \qquad n_{p-1} < k \leqq n_p, \qquad (p = 1, 2, \cdots)$$
$$\sigma_{\nu_p} > p - 1/p; \qquad \sigma_{n_p} < -p \qquad (p = 1, 2, \cdots).$$

It is easy to see that $s_n \to +\infty$, and that the core Γ of σ_n is the entire real axis. This proves Lemma 3. 5, and Theorem 3. 1 follows.

In proving Theorem 3. 1, we showed that if A is regular and (3. 11) fails, then there is a sequence s_n for which $\mathcal{R}(s_n) \to +\infty$ while $\sigma_n \sim \infty$ fails. This observation, together with the fact that $\mathcal{R}(s_n) \to \infty$ implies $s_n \sim \infty$, gives

THEOREM 3. 6. *In order that a regular matrix A may have the property that $\mathcal{R}(s_n) \to +\infty$ implies $\sigma_n \sim \infty$, it is necessary and sufficient that an index K exist for which*

$$(3.61) \qquad a_{nk} = \mathcal{R}(a_{nk}) \geqq 0 \qquad k \geqq K.$$

It appears from Theorems 3. 1 and 3. 6 (and can be shown directly with the aid of Theorem 2. 1) that the class of regular matrices for which $\mathcal{R}(s_n) \to +\infty$ implies $\sigma_n \sim \infty$ is identical with the class of regular matrices for which $s_n \sim \infty$ implies $\sigma_n \sim \infty$.

The condition (3. 61) is not necessary in order that a regular transformation be such that $s_n = \mathcal{R}(s_n) \to +\infty$ implies $\sigma_n \sim \infty$. This is shown (for example) by the simple regular transformation

$$(3.62) \qquad \sigma^*_n = (1 + i/n)s_n$$

whose matrix is a diagonal matrix. It is clear that if $s_n = \mathcal{R}(s_n) \to +\infty$, then $\mathcal{R}(\sigma^*_n) = s_n \to +\infty$ and hence $\sigma_n \sim \infty$.

4. Theorem on cores. The next theorem is on the one hand a slight extension of Knopp's Kernsatz, and on the other hand a converse of the extension.

THEOREM 4. 1. *In order that a regular transformation A, determined by a matrix a_{nk} of complex constants, may be such that the core C of each sequence s_n contain the core Γ of its transform σ_n, it is necessary and sufficient that an index K exist for which*

$$(4.11) \qquad a_{nk} = \mathcal{R}(a_{nk}) \geqq 0 \qquad k \geqq K.$$

Sufficiency is asserted by Lemma 3.2. To prove necessity, we observe that if (4.11) fails, then by Theorem 3.1 there is a sequence s_n for which C is empty while Γ contains at least one point so that $\Gamma \subset C$ fails.

In our proof of Theorem 4.1 we showed that if (4.11) fails, then there is an *unbounded* sequence s_n whose core does not contain the core of the transform of s_n. It is not true that failure of (4.11) necessarily implies existence of a *bounded* sequence s_n whose core does not contain the core of the transform of s_n. In fact, in the case of (3.62), (4.11) fails and the core of each bounded sequence is identical with the core of its transform.

THEOREM 4.2. *In order that a regular transformation A, determined by a matrix a_{nk} of complex constants, may be such that the core C of each* BOUNDED *sequence s_n contain the core Γ of its transform σ_n, it is necessary and sufficient that*

$$\lim_{n\to\infty} \sum_{k=1}^{n} | a_{nk} | = 1. \tag{4.21}$$

It is known [5] that, for a regular transformation A, (4.21) is necessary and sufficient to ensure that

$$\limsup_{m,n\to\infty} | \sigma_m - \sigma_n | \leqq \limsup_{m,n\to\infty} | s_m - s_n |$$

for each bounded sequence s_n. Necessity follows from this. To prove sufficiency, let A be regular, let (4.21) hold, and let $| s_n | < M$. Let $a_{nk} = b_{nk} + ic_{nk}$ where a_{nk} and b_{nk} are real; and let $b_{nk} = b^+_{nk} + b^-_{nk}$ where

$$b^+_{nk} = (b_{nk} + | b_{nk} |)/2 \geqq 0 \quad \text{and} \quad b^-_{nk} = (b_{nk} - | b_{nk} |)/2 \leqq 0.$$

Let

$$\sigma_n = \sum_{k=1}^{n} a_{nk}s_k, \qquad \sigma'_n = \sum_{k=1}^{n} b^+_{nk}s_k.$$

Then (W. A. Hurwitz, *loc. cit.*, pp. 615-616) the matrix b^+_{nk} is regular and

$$\lim_{n\to\infty} \sum_{k=1}^{n} | b^-_{nk} | = 0; \qquad \lim_{n\to\infty} \sum_{k=1}^{n} | c_{nk} | = 0.$$

Hence the core C of s_n contains the core Γ' of σ'_n; and

$$| \sigma_n - \sigma'_n | \leqq M \sum_{k=1}^{n} | b^-_{nk} | + M \sum_{k=1}^{n} | c_{nk} | \to 0$$

implies that the core Γ of σ_n coincides with the core Γ'. Therefore $C \supset \Gamma$ and sufficiency is proved.

5. Theorems of Steinhaus type. The following theorem is a generalization of a theorem of Steinhaus (§ 1). It implies (among other things) that

[5] W. A. Hurwitz, "The oscillation of a sequence," *American Journal of Mathematics*, vol. 52 (1930), pp. 611-616.

it is impossible to specialize a regular transformation A and a core C of a sequence s_n in such a way that the core Γ of the transform σ_n must be a proper subset of C.

THEOREM 5. 1. *If A is regular and E is a closed non-empty point set in the complex plane, then there is a sequence s_n of points of E such that the set E_s of limit points of s_n coincides with E and the set E_σ of limit points of σ_n contains E, i. e. $E_\sigma \supset E_s = E$.*

Let $\alpha_1, \alpha_2, \cdots$ be a sequence whose elements form a subset of E dense in E. Let the elements of the sequence

$$\alpha_1, \alpha_1, \alpha_2, \alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_1, \alpha_2, \cdots, \alpha_n, \cdots$$

be denoted in order by $\beta_1, \beta_2, \cdots$. Let n_1 be an index such that

$$|\, \beta_1 - \sum_{k=1}^{n_1} a_{n_1 k}\beta_1 \,| < 2^{-1},$$

and put $s_k = \beta_1$ when $1 \leqq k \leqq n_1$. In general, when $n_1 < n_2 < \cdots < n_{p-1}$ are defined, and s_k is defined for $1 \leqq k \leqq n_{p-1}$, choose $n_p > n_{p-1}$ such that

$$|\, \beta_p - \sum_{k=1}^{n_{p-1}} a_{n_p k} s_k - \sum_{k=n_{p-1}+1}^{n_p} a_{n_p k}\beta_p \,| < 2^{-p},$$

and put $s_k = \beta_p$ when $n_{p-1} < k \leqq n_p$. With the sequence s_n defined thus by induction, we observe that $|\, \beta_p - \sigma(n_p) \,| < 2^{-p}$ and that s_n and σ_n have the requisite properties to establish Theorem 5. 1.

In case the set E of Theorem 5. 1 is convex as well as closed and non-empty, the core C of the sequence s_n constructed in the proof of Theorem 5. 1 is the set E and we have $\Gamma \supset E_\sigma \supset E_s = C = E$. If moreover A is regular and satisfies (4. 11), then we have $\Gamma \subset C$ as well as $\Gamma \supset C$. These remarks prove

THEOREM 5. 2. *If A is regular and satisfies the condition*

$$a_{nk} = \Re\,(a_{nk}) \geqq 0 \qquad k \geqq K, \tag{5. 21}$$

then, corresponding to each closed convex non-empty set E in the complex plane, there is a sequence s_n such that the core C of s_n and the core Γ of its transform σ_n both coincide with E, i. e. $\Gamma = C = E$.

It follows from Theorems 4. 2 and 5. 1 that Theorem 5. 2 holds when (5. 21) is replaced by (4. 21) and the sets E considered are bounded as well as convex, closed, and non-empty.

CORNELL UNIVERSITY,
ITHACA, N. Y.

NON-LINEAR ALGEBRAIC DIFFERENCE EQUATIONS WITH FORMAL SOLUTIONS OF THE SAME TYPE AS THE FORMAL SOLUTIONS OF LINEAR HOMOGENEOUS DIFFERENCE EQUATIONS.* [1]

By Otis E. Lancaster.

Here, we consider the following problem: Given a non-linear algebraic difference equation

$$(1) \qquad F(x, y(x), y(x+1), \cdots, y(x+m)) = 0,$$

where F is a polynomial with rational coefficients in its arguments x, $y(x)$, $y(x+1), \cdots, y(x+m)$. What is the nature of F when the equation has a solution in common with that of a linear homogeneous algebraic difference equation? Or more generally, what is the nature of F when (1) has a formal solution of the same general type as that of the formal solutions of linear homogeneous algebraic difference equations? That is, what are the properties of F when (1) has a formal solution of the form [2]

$$(2) \qquad y(x) = x^{ax} b^x x^d e^{L^{(p)}(x)} \cdot R(x^{-(1/p)}),$$

where

$$L^{(p)}(x) = \delta_1 x^{(p-1)/p} + \delta_2 x^{(p-2)/p} + \cdots + \delta_{p-1} x^{1/p},$$
$$R(x^{-(1/p)}) = s_0 + s_1 x^{-(1/p)} + s_2 x^{-(2/p)} + \cdots.$$

p is a positive integer and ap is an integer? And, how many solutions of this type may a given equation possess?

First, we state an obvious theorem.

Theorem 1. *A non-linear algebraic difference equation cannot have a formal solution* (2) *which does not cause each of the homogeneous parts to vanish identically, unless* $a = 0$, $\delta_i = 0$ $(i = 1, 2, \cdots, p-1)$ *and* $b = 1$.

This theorem permits us to divide the problem into two cases, with regard to the vanishing or non-vanishing of the homogeneous parts of (1) when $y(x)$ is replaced by (2).

* Received January 11, 1938.

[1] The thanks of the author are due to Professor G. D. Birkhoff for suggestions furnished by him during the preparation of this paper.

[2] G. D. Birkhoff, "Formal theory of irregular linear difference equations," *Acta Mathematica*, vol. 54 (1930), pp. 205-246.

Case I. The series (2) *makes the homogeneous parts of* (1) *vanish identically.*

We treat this case by considering only homogeneous equations, remembering that when the equation is non-homogeneous the same properties must hold for each homogeneous part thereof.

1. Equations satisfied by all solutions of linear equations.

THEOREM 2. *If a non-linear homogeneous algebraic difference equation of the m-th order is satisfied by all the solutions of a linear difference equation*

$$\sum_{i=0}^{l} a_i(x)y(x+i)=0, \qquad (l\leq m), \tag{3}$$

where $a_0(x), a_1(x), \cdots, a_l(x)$ *are polynomials in* x*, then, it may be written in the form*

$$\sum_{j=0}^{m-l}[\sum_{i=0}^{l}a_i(x+j)y(x+i+j)]\Phi_j(x,y(x),y(x+1),\cdots,y(x+l+j))=0, \tag{4}$$

where $\Phi_0, \Phi_1, \cdots, \Phi_{m-l}$ *are homogeneous polynomials in the y's, whose coefficients are rational functions of* x.

Proof. When $m\geq l$, any non-linear algebraic difference equation may be written in the form

$$\begin{aligned}\sum_{j=0}^{m-l}[\sum_{i=0}^{l}a_i(x+j)y(x+i+j)]\Phi_j(x,y(x),\cdots,y(x+l+j))\\ +\Psi(x,y(x),\cdots,y(x+l-1))=0,\end{aligned} \tag{5}$$

where $\Phi_0, \Phi_1, \cdots, \Phi_{m-l}$ and Ψ are homogeneous polynomials in the y's, whose coefficients are rational functions of x with poles congruent to the zeros of $a_l(x)$. The first part of (5) vanishes at all points incongruent to the zeros of $a_l(x)$ for every solution of (3). So, when the general solution of (3) is a solution of (5) it must satisfy, at all points incongruent to the zeros of $a_l(x)$, the difference equation

$$\Psi(x,y(x),\cdots,y(x+l-1))=0. \tag{6}$$

This is only possible when the coefficients of Ψ vanish identically in x, for the general solution of the non-linear difference equation (6) contains fewer arbitrary parameters than the general solution of the linear equation (3). Q. E. D.

COROLLARY 2.1. *A first order non-linear homogeneous algebraic difference equation,* $F(x,y(x),y(x+1))=0$*, is satisfied by all of the solutions*

of a first order linear difference equation $y(x+1) - a(x)y(x) = 0$, *where* $a(x)$ *is a rational function, if and only if* $y(x+1) - a(x)y(x)$ *is a factor of* $F(x, y(x), y(x+1))$.

It follows immediately from the corollary that it is always possible to form a first order difference equation of the q-th degree which is satisfied by all solutions of q distinct first order linear difference equations, and, in general, that a first order homogeneous equation of the q-th degree is satisfied by all the solutions of the q linear equations formed by setting the factors equal to zero. But the problem of determining the linear equations whose general solutions satisfy a given non-linear difference equation of higher than first order, is not a simple factoring problem, since $\sum_{i=0}^{l} a_i(x)y(x+i)$ may not be a factor of $F(x, y(x), \cdots, y(x+m))$. The following questions naturally arise: How many distinct linear difference equations of the first order have solutions which satisfy a given non-linear difference equation? May this number ever be infinite? If infinite, what are the special characteristics of the equations?

From a formal standpoint the first of the above questions may be stated in the following manner: How many linearly independent formal solutions (2) satisfy a non-linear homogeneous difference equation?

After Theorem 2 it is clear that if a non-linear difference equation is satisfied by all solutions of a linear equation, it is also satisfied by all the formal solutions of the linear equation. However, since it is not known that all formal solutions of a non-linear difference equation are asymptotic representations of actual solutions, the number of linearly independent formal solutions (2) is greater than or equal to the number of linearly independent solutions that satisfy homogeneous linear equations. We hope to show later that these two are equal, but at present we concentrate only on the formal part.

2. Formal series solutions. We consider in detail the conditions which are sufficient to insure that a non-linear difference equation of q-th degree and the m-th order,

$$\sum_{i_1, i_2, \ldots, i_q = 0}^{m} x^{k_{i_1 i_2 \cdots i_q}} \left[a_{0 i_1 i_2 \ldots i_q} + \frac{a_{1 i_1 i_2 \ldots i_q}}{x} + \cdots \right] y(x+i_1)y(x+i_2) \cdots y(x+i_q) = 0, \tag{7}$$

is formally satisfied by an expression of the form (2). If

$$y(x) = x^{ax} b^x x^d e^{L^{(p)}(x)} R(x^{-(1/p)}), \tag{2}$$

then

$$
\begin{aligned}
(9)\quad y(x+i) = {} & x^{ax+ai+d} b^{x+i} e^{ai}\left(1+\frac{ai^2}{2x}+\cdots\right) e^{L^{(p)}(x)} \\
& \cdot\left[1+\frac{di}{x}+\frac{d(d-1)}{2!}\,\frac{i^2}{x^2}+\cdots\right] \\
& \cdot\left[1+\frac{\delta_1(p-1)i}{px^{1/p}}+\frac{\delta_1{}^2(p-1)^2i^2}{2!\,p^2x^{2/p}}+\cdots+\frac{\delta_1{}^p(p-1)^p i^p}{p!\,p^p x}\right. \\
& \left.+\left(\frac{\delta_1{}^{p+1}(p-1)^{p+1}i^{p+1}}{(p+1)!\,p^{p+1}}+\frac{\delta_1(p-1)(-1)i^2}{p^2\cdot 2!}\right)\frac{1}{x^{(1+p)/p}}+\cdots\right] \\
& \cdots\left[1+\frac{\delta_{p-1}}{p}\,\frac{i}{x^{(p-1)/p}}+\frac{\delta^2{}_{p-1}i^2}{p^2 2!}\cdot\frac{1}{x^{(2p-2)/p}}+\cdots\right] \\
& \cdot\left[s_0+\frac{s_1}{x^{1/p}}+\frac{s_2}{x^{2/p}}+\cdots+\frac{s_p}{x}+\frac{s_{p+1}-\frac{i}{p}s_1}{x^{(p+1)/p}}\right. \\
& +\frac{s_{p+2}-\frac{2i}{p}s_2}{x^{(p+2)/p}}+\cdots+\frac{s_{2p}-is_p}{x^2} \\
& \left.+\frac{s_{2p+1}-\frac{p+1}{p}is_{p+1}+\frac{1}{p}\left(\frac{1+p}{p}\right)\frac{i^2}{2!}s_1}{x^{(2p+1)/p}}+\cdots\right],
\end{aligned}
$$

since formally

$$
\begin{aligned}
(x+i)^{a(x+i)} & = x^{ax+ia}(1+i/x)^{ia}(1+i/x)^{ax} \\
& = x^{ax+ia}(1+i/x)^{ia}e^{ax\log(1+i/x)} \\
& = x^{ax+ia}(1+i/x)^{ia}e^{ax(i/x-i^2/x^2+i^3/3x^3+\ldots)} \\
& = x^{ax+ia}\left(1+\frac{ai^2}{x}+\frac{(ia-1)ia}{2!}\,\frac{i^2}{x^2}+\cdots\right) \\
& \qquad\times e^{ai}\left[1-\frac{ai^2}{2x}+\left(\frac{ai^3}{3}+\frac{a^2i^4}{8}\right)\frac{1}{x^2}+\cdots\right] \\
& = x^{ax+ia}e^{ia}\left[1+\frac{ai^2}{2x}+\left(\frac{a^2i^4}{8}-\frac{ai^3}{6}\right)\frac{1}{x^2}+\cdots\right],
\end{aligned}
$$

$$
\begin{aligned}
e^{\delta_j(x+i)^{(p-j)/p}} & = e^{\delta_j x^{(p-j)/p}(1+i/x)^{(p-j)/p}} \\
& = e^{\delta_j x^{(p-j)/p}[1+(p-j)/p\,.\,i/x+((p-j)/p)((-j)/p)(i^2/2!\,x^2)+\ldots]} \\
& = e^{\delta_j x^{(p-j)/p}}\left[1+\delta_j\frac{(p-j)}{p}\cdot\frac{i}{x^{j/p}}+\frac{\delta_j{}^2(p-1)^2i^2}{2!\,p^2x^{2j/p}}\right. \\
& \qquad\left.+\frac{\delta_j{}^3(p-j)^3i^3}{3!\,p^3x^{3j/p}}+\cdots+\delta_j\left(\frac{p-j}{p}\right)\left(\frac{-j}{p}\right)\frac{i^2}{2!\,x^{(j+p)/p}}+\cdots\right]
\end{aligned}
$$

and

$$
\frac{s_j}{(x+i)^j}=\frac{s_j}{x^j}\left(1+\frac{i}{x}\right)^{-j}=\frac{s_j}{x^j}\left(1-\frac{ji}{x}+\frac{j(j-1)}{2!}\,\frac{i^2}{x^2}+\cdots\right).
$$

Hence,

$$(10)\quad y(x+i_1)y(x+i_2)\cdots y(x+i_q)$$
$$= x^{q(ax+d)+a(i_1+i_2+\cdots+i_q)}b^{qx+(i_1+i_2+\cdots+i_q)}e^{a(i_1+i_2+\cdots+i_q)}$$
$$\cdot\, e^{qL^{(p)}(x)}\cdot A(x)\cdot\Delta_1(x)\cdot\cdots\cdot\Delta_{p-1}(x)\cdot D(x)\cdot S(x,p),$$

where

$$A(x)=\Big[1+\frac{a(i_1^2+i_2^2+\cdots+i_q^2)}{2x}+\Big\{\frac{a^2(i_1^2+i_2^2+\cdots+i_q^2)^2}{8}$$
$$-\frac{a(i_1^3+i_2^3+\cdots+i_q^3)}{6}\Big\}\frac{1}{x^2}+\cdots\Big];$$

$$\Delta_1(x,p)=\Big[1+\frac{\delta_1(p-1)(i_1+i_2+\cdots+i_q)}{px^{1/p}}$$
$$+\frac{\delta_1^2(p-1)^2(i_1+i_2+\cdots+i_q)^2}{2!\,p^2x^{2/p}}$$
$$+\cdots+\frac{\delta_1^p(p-1)^p(i_1+i_2+\cdots+i_q)^p}{p!\,p^px}$$
$$+\Big\{\frac{\delta_1^{p+1}(p-1)^{p+1}}{(p+1)!\,p^{p+1}}(i_1+i_2+\cdots+i_q)^{p+1}$$
$$+\frac{\delta_1(p-1)(-1)}{p^2 2!}(i_1^2+i_2^2+\cdots+i_q^2)\Big\}\frac{1}{x^{(p+1)/p}}+\cdots\Big];$$

. . . .

$$\Delta_{p-1}(x,p)=\Big[1+\frac{\delta_{p-1}(i_1+i_2+\cdots+i_q)}{x^{(p-1)/p}}+\frac{\delta^2_{p-1}(i_1+i_2+\cdots+i_q)^2}{p^p 2!\,x^{(2p-2)/p}}$$
$$+\frac{\delta_{p-1}\left(\frac{1}{p}\right)\left(\frac{1-p}{p}\right)(i_1^2+i_2^2+\cdots+i_q^2)}{2!\,x^{(2p-1)/p}}+\cdots\Big];$$

$$D(x)=\Big[1+\frac{d(i_1+i_2+\cdots+i_q)}{x}+\Big\{\frac{d^2(i_1+i_2+\cdots+i_q)^2}{2!}$$
$$-\frac{d(i_1^2+i_2^2+\cdots+i_q^2)}{2!}\Big\}\frac{1}{x^2}+\cdots\Big]$$

and

$$S(x,p)=s_0^q+\frac{qs_1s_0^{q-1}}{x^{1/p}}+\frac{qs_0^{q-1}s_2+\frac{q(q-1)}{2!}s_0^{q-2}s_1^2}{x^{2/p}}+\cdots$$
$$+\frac{qs_0^{q-1}s_p+q(q-1)s_{p-1}s_1s_0^{q-2}+\cdots}{x}$$
$$+\frac{qs_{p+1}s_0^{q-1}-(i_1+i_2+\cdots+iq)s_1s_0^{q-1}+q(q-1)s_ps_1s_0^{q-2}+\cdots}{x^{(p+1)/p}}$$
$$+\frac{qs_{p+1}s_0^{q-1}-\frac{2(i_1+i_2+\cdots+i_q)}{p}s_2s_0^{q-1}+q(q-1)s_{p+1}s_1s_0^{q-2}+\cdots}{x^{(p+2)/p}}+\cdots$$
$$qs_{2p}s_0^{q-1}-(i_1+i_2+\cdots+i_q)s_ps_0^{q-1}+q(q-1)s_{2p-1}s_1s_0^{q-2}$$

$$+\frac{-\frac{(p-1)(i_1+i_2+\cdots+i_q)}{p}s_{p-1}s_1s_0^{q-2}+\cdots}{x^2}$$

$$+\frac{qs_{2p+1}s_0^{q-1}-\frac{p+1}{p}(i_1+i_2+\cdots+i_q)s_{p+1}s_0^{q-1}+\frac{1}{p}\left(\frac{1}{p}+1\right)\frac{(i_1^2+i_2^2+\cdots+i_q^2)}{2!}s_1s_0^{q-1}+\cdots}{x^{(2p+1)/p}}$$

$$+\cdots.$$

When we substitute the expression (10) in equation (7) and remove the common factor $x^{q(ax+d)}b^{qx}e^{qL^{(p)}(x)}$, the leading terms of the $(m+1)^q$ series are of the form

$$a_{0i_1i_2\ldots i_q}x^{k_{i_1i_2\ldots i_q}+a(i_1+i_2+\ldots+i_q)}.$$

If the relation is a formal identity, then there must be two leading terms of the same degree in x; while all other terms are not of higher degree; that is,

$$k_{i_1i_2\ldots i_q}+a(i_1+i_2+\cdots+i_q)=k_{j_1j_2\ldots j_q}+a(j_1+j_2+\cdots+j_q)$$

for some values of $i_1, i_2, \cdots, i_q$ and $j_1, j_2, \cdots, j_q$, where not all of the values $i_1, i_2, \cdots, i_q$ are equal to the values $j_1, j_2, \cdots, j_q$ respectively; and

$$k_{l_1l_2\ldots l_q}+a(l_1+l_2+\cdots+l_q)\leqq k_{j_1j_2\ldots j_q}+a(j_1+j_2+\cdots+j_q)$$
$$[l_1, l_2, \cdots, l_q=0, 1, 2, \cdots, m].$$

Expressing these two relations in another manner, we have

$$a=-\frac{k_{i_1i_2\ldots i_q}-k_{j_1j_2\ldots j_q}}{(i_1+i_2+\cdots+i_q)-(j_1+j_2+\cdots+j_q)} \tag{11}$$

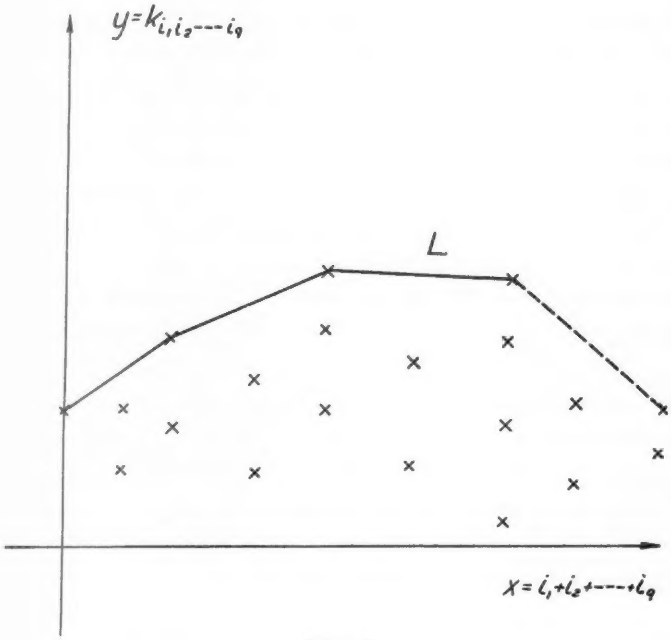
and

$$k_{l_1l_2\ldots l_q}-k_{j_1j_2\ldots j_q}\leqq -a[(l_1+l_2+\cdots+l_q)-(j_1+j_2+\cdots+j_q)] \tag{12}$$
$$(l_1, l_2, \cdots, l_m=0, 1, 2, \cdots, m).$$

These conditions admit a simple geometric representation. For, if we plot the points $(i_1+i_2+\cdots+i_q,\ k_{i_1i_2\ldots i_q})$, where $i_1+i_2+\cdots+i_q$ is taken along the horizontal axis and $k_{i_1i_2\ldots i_q}$ along the vertical axis, the conceivable values of a are given by the negative of the slopes of all possible lines joining two of these points, while the inequality (12) will only hold if the other points lie below or on a line whose equation is

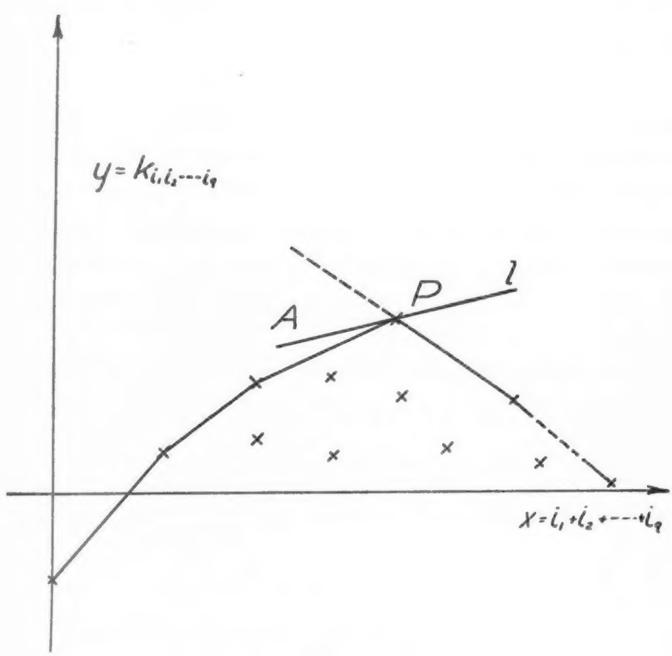
$$y-k_{j_1j_2\ldots j_q}=-a[x-(j_1+j_2+\cdots+j_q)]$$

(see Figure 1). This leads to a broken line L, concave downwards, whose vertices fall at certain of these points, while all other points lie below or on this line L.



$y = k_{i_1 i_2 \cdots i_q}$
L
$x = i_1 + i_2 + \cdots + i_q$

FIG. 1.



$y = k_{i_1 i_2 \cdots i_q}$
A
P
l
$x = i_1 + i_2 + \cdots + i_q$

FIG. 2.

It is important to note that in the above diagram two or more points may coincide, since several points may have the same abscissa. In this respect it is unlike the diagram used by Birkhoff in his development of the formal theory of linear difference equations.[2] If the diagram has a "*multiple point vertex*," that is, if two or more points $(k_{i_1 i_2 \ldots i_q}, i_1 + i_2 + \cdots + i_q)$ coincide at a vertex, then the negative of the slope of any line l passing through the point, such that all other points lie below l, is an admissible value for a. Hence, all values of an interval give possible values for a. For example, if P is a multiple point vertex, (see Figure 2) then the negatives of all the slopes of the lines passing through P and the region A give admissible values for a. The diagram for a difference equation of the m-th order and the q-th degree may have $mq - 3$ multiple point vertices. Hence it is possible to have $mq - 3$ intervals of values for a. If none of the vertices of the Puiseux diagram are multiple points, then the negatives of the slopes of the line segments of L determine uniquely all the allowable values for a.

There is always at least one value for a, for a linear equation, but this is not true for every non-linear equation. For if all

$$a_{v i_1 i_2 \ldots i_q} = 0 \qquad (v = 0, 1, 2, 3, \cdots)$$

except, when $i_1 + i_2 + \cdots + i_q = K$, where K is an integer, and if, the values $k_{i_1 i_2 \ldots i_q}$ are all distinct, then the line in the Puiseux diagram which connects these points is vertical. Hence there is no finite value for a. In all other cases there is at least one a.

THEOREM 3. *If $i_1 + i_2 + \cdots + i_q = K$ for all terms of a homogeneous algebraic difference equation and if all the exponents $k_{i_1 i_2 \ldots i_q}$ are distinct, then there is no formal solution of the form* (2).

When a vertex of the Puiseux diagram is a multiple point, a may have irrational values, but, since irrational values of a do not yield formal solutions of a linear difference equation, they are excluded from the remainder of the discussion.

When $a = c/h$ is a rational number, if we take $p = h$ and divide the supposed identity (formed by substituting (10) in equation (7)) by the highest power of x, i. e.

$$x^{k_{j_1 j_2 \ldots j_q} + a(j_1 + j_2 + \cdots + j_q)},$$

then our relation becomes

$$(13) \quad \sum_{i_1=0,\, i_2=0, \ldots,\, i_q=0}^{m} \left(a'_{0 i_1 i_2 \ldots i_q} + \frac{a'_{1 i_1 i_2 \ldots i_q}}{x^{1/h}} + \frac{a'_{2 i_1 i_2 \ldots i_q}}{x^{2/h}} + \cdots + \frac{a'_{h i_1 i_2 \ldots i_q}}{x} + \cdots \right) \cdot$$

$$b^{i_1 + i_2 + \cdots + i_q} e^{a(i_1 + i_2 + \cdots + i_q)} \cdot A(x) \cdot \Delta_1(x, h) \cdot \Delta_2(x, h) \cdot \cdots \cdot \Delta_{p-1}(x, h) \cdot D(x) \cdot S(x, h) \equiv 0,$$

where, when $\frac{w_{i_1 i_2 \ldots i_q}}{h}$ is the difference in degree of the term $x^{k_{i_1 i_2 \ldots i_q} + a(i_1+i_2+\ldots+i_q)}$ and the term of highest degree,

$$(14) \quad a'_{n i_1 i_2 \ldots i_q} = a_{\left(\frac{n - w_{i_1 i_2 \ldots i_q}}{h}\right) i_1 i_2 \ldots i_q}, \; n \geqq w, \; n - w = rh \quad (r = 0, 1, 2, 3, \cdots)$$

$$= 0, \qquad n - w \neq rh \quad (r = 0, 1, 2, 3, \cdots)$$

$$(n = 0, 1, 2, 3, \cdots).$$

Since the equation (13) is a formal identity, the coefficient of the powers of $1/x$ must vanish. If we let

$$(15) \qquad f(b) = \sum_{i_1=0,\, i_2=0, \ldots,\, i_q=0}^{m} b^{i_1+i_2+\ldots+i_q} e^{a(i_1+i_2+\ldots+i_q)} a'_{0 i_1 i_2 \ldots i_q}$$

and equate the constant term of (13) to zero, we have

$$f(b) s_0^q = 0.$$

Hence,

$$(16) \qquad f(b) = 0.$$

This equation determines the values of b, we shall call it the "*characteristic equation.*" There is a characteristic equation for each rational value of a. When the vertices of the Puiseux diagram are not multiple points, then, as stated above, the values of a are uniquely determined. If we denote these values by $a_1, a_2, \cdots, a_n$, where $a_1 > a_2 > \cdots > a_n$, then, the total number of non-zero values for b (counting the roots according to their multiplicity in the separate equations) is precisely ν, where ν is the difference in the maximum and minimum values of the sum $i_1 + i_2 + \cdots + i_q$. For if $x_0, x_1, \cdots, x_n$ are the values of x for the successive vertices the number of roots of the n characteristic equations corresponding to $a_1, a_2, \cdots, a_n$ are $x_1 - x_0$, $x_2 - x_1$, $\cdots$, $x_n - x_{n-1}$ respectively.

When the Puiseux diagram has a multiple point at $x = x_r$, then in addition to the m characteristic equations mentioned above there is another, viz.,

$$(17) \qquad b^{x_r} \sum_{i_1+i_2+\ldots+i_q=x_r} a'_{0 i_1 i_2 \ldots i_q} = 0$$

(the summation is to be taken over all values $i_1, i_2, \cdots, i_q$ such that their sum equals x_r). This equation does not have any non-zero roots, unless

$$\sum_{i_1+i_2+\ldots+i_q=x_r} a'_{0 i_1 \ldots i_q} = 0$$

and then it is satisfied by any value. Hence, if

$$\sum_{i_1+i_2+\ldots+i_q=x_r} a'_{0 i_1 i_2 \ldots i_q} \neq 0$$

for the abscissas of each multiple point vertex of the Puiseux diagram, then again, the number of non-zero values for b is precisely the difference between the maximum and the minimum values of the sum $i_1 + i_2 + \cdots + i_q$. We call $\phi_1(b, a) = 0$ the *secondary equation*, $\phi_2(b, a) = 0$ the tertiary equation, $\cdots$; where

$$(18)\quad \phi_j(b, a) = \sum_{i_1=0,\, i_2=0, \ldots,\, i_q=0}^{m} a''_{j i_1 i_2 \ldots i_q} b^{i_1+i_2+\cdots+i_q} e^{a(i_1+i_2+\cdots+i_q)} \qquad (j = 1, 2, 3, \cdots),$$

and the $a''_{j i_1 i_2 \ldots i_q}$'s are the coefficients of the powers of $x^{-(j/p)}$ in the product

$$A(x) \cdot \left[a'_{0 i_1 i_2 \ldots i_q} + \frac{a_{1 i_1 i_2 \ldots i_q}}{x^{1/p}} + \cdots \right].$$

If b_1 is a root of the characteristic equation, $f(b) = 0$, when the coefficient of $x^{-(1/h)}$ in (13) is set equal to zero, we have

$$\delta_1 \frac{h-1}{h} b_1 f'(b_1) = -\phi_1(b_1, a).$$

This equation uniquely determines δ_1 when b_1 is not a multiple root of $f(b) = 0$. But when b_1 is a multiple root of $f(b) = 0$, δ_1 does not exist unless b_1 is also a root of the secondary equation.

Equating the coefficients of $x^{-(j/p)}$ to zero, we obtain the equations

$$\delta_j \frac{h-j}{h} b_1 f'(b_1) = -\phi_j(b_1, a) + \psi_j(\delta_1, \delta_2, \cdots, \delta_{j-1}) \qquad (j = 2, 3, \cdots, h-1).$$

$$d b_1 f'(b_1) = -\phi_h(b_1, a) + \psi_h(\delta_1, \delta_2, \cdots, \delta_{h-1})$$

$$\frac{s_{j-h}}{s_0} \left[-\frac{j-h}{h} b_1 f'(b_1) \right] = -\phi_j(b_1, a) + \psi_j\left(\delta_1, \delta_2, \cdots, \delta_{h-1}, d, \frac{s_1}{s_0}, \cdots, \frac{s_{j-h-1}}{s_0} \right) \qquad (j = h+1, h+2, \cdots),$$

which determine in order the δ_j $(j = 2, 3, \cdots, h-1)$, d and the ratios s_{j-h}/s_0 $(j = h+1, h+2, \cdots)$ provided $b_1 f'(b_1) \neq 0$.

Thus we have established the following theorem.

THEOREM 4. *If $i_1 + i_2 + \cdots + i_q$ is not equal to the same constant for all terms of a homogeneous algebraic difference equation, and if one of the characteristic equations has a simple non-zero root, then the equation has a formal solution of the form* (2).

The above theorem was stated so as to insure the existence of at least one a and one b. When an a exists there may be no non-zero values for b, hence no formal solutions of the desired type.

THEOREM 5. *If* $i_1 + i_2 + \cdots + i_q = K$ *for all terms of an homogeneous algebraic difference equation, and if, two or more of the leading exponents* $k_{i_1 i_2 \ldots i_q}$ *are equal, and if* $\sum_{i_1+i_2+\ldots+i_q=K} a'_{0 i_1 i_2 \ldots i_q} \neq 0$ *then, the equation does not have a formal solution of the form* (2).

3. Regular equations. Before stating the other results that are evident from the above consideration, it is convenient to make the following definition.

DEFINITION. *A homogeneous algebraic difference equation is "regular" if the roots of each of the* n *characteristic equations are distinct and if the Puiseux diagram does not have a multiple point vertex at* $x = x_r$ *for which* $\sum_{i_1+i_2+\ldots+i_q=x_r} a'_{0 i_1 i_2 \ldots i_q} = 0$.

THEOREM 6. *A regular homogeneous algebraic difference equation has* ν *and only* ν *linearly independent formal solutions* (2), *where* ν *is the difference between the maximum and minimum values of the sum* $i_1 + i_2 + \cdots + i_q$.

COROLLARY 6. 1. *A regular homogeneous algebraic difference equation of the m-th order and the q-th degree which contains both of the terms* $c_1(x)[y(x+m)]^q$ *and* $c_2(x)[y(x)]^q$, $c_1(x)c_2(x) \not\equiv 0$ *has* mq *and only* mq *linearly independent formal solutions of the form* (2).

4. Cases where the characteristic equations have multiple roots. Now let us consider the case where b_1 is a root of the characteristic equation of multiplicity $\omega > 1$, but is not a root of the secondary equation. If $a = c/h$ it is clear from the preceding work that a series (2) in which $p = h$ cannot formally satisfy the difference equation. Hence, if there are solutions of the form (2) corresponding to b_1 then p must have some other value. We set $p = \omega h$ and replace $y(x)$ by the expression (2). After the highest common factor has been removed, the relation is

$$
(19) \quad \sum_{i_1=0,\, i_2=0,\, \ldots,\, i_q=0}^{m} \left(a'_{0 i_1 i_2 \ldots i_q} + \frac{a'_{1 i_1 i_2 \ldots i_q}}{x^{1/h}} + \cdots \right) (e^a b)^{i_1+i_2+\cdots+i_q}
$$
$$
\cdot A(x) \cdot \Delta_1(x, \omega h) \cdot \Delta_2(x, \omega h) \cdot \cdots \cdot \Delta_{\omega h - 1}(x, \omega h) \cdot D(x) \cdot S(x, \omega h) = 0,
$$

where the a''s have the same meaning as before.

Before proceeding to show that the coefficients of the series exist, we prove a lemma.

LEMMA.

$$
(20) \quad \sum_{i_1=0,\, i_2=0,\, \ldots,\, i_q=0}^{m} (i_1 + i_2 + \cdots + i_q)^r (e^a b)^{i_1+i_2+\cdots+i_q} a'_{0 i_1 i_2 \ldots i_q} = \sum_{i=1}^{r} c_i b^i f^{(i)}(b)
$$

where $c_r = 1$ and the other c_i's are integers and $f(b) = 0$ is the characteristic equation (16).[3]

Proof. This is obviously true for $r = 1$. Assume it is true for $r - 1$. If we set $i_1 + i_2 + \cdots + i_q = j$ then by definition

$$b^r f^{(r)}(b) = \sum_{i_1=0,\, i_2=0,\ldots,\, i_q=0}^{m} j(j-1)\cdots(j-r+1)c'_{0j}b^j e^{aj},$$

(where $c_{0j} = \sum_{i_1+i_2+\ldots+i_q=j} a'_{0i_1\ldots i_q}$) or

$$b^r f^{(r)}(b) = \sum_{i_1=0,\, i_2=0,\ldots,\, i_q=0}^{m} \left(j^r - \frac{(r-1)r}{2} j^{r-1} + \cdots + (-1)^{r-1}(r-1)!\,j\right) c'_{0j}b^j e^{aj}.$$

Therefore,

$$\sum_{i_1=0,\, i_2=0,\ldots,\, i_q=0}^{m} j^r a'_{0j} b^j e^{aj} = b^r f^{(r)}(b) + \sum_{i_1=0,\, i_2=0,\ldots,\, i_q=0}^{m} \left[\frac{r(r-1)}{2} j^{r-1} - \cdots + (-1)^r (r-1)!\,j\right] b^j e^{aj} c'_{0j}$$

and after the assumption the right member equals

$$b^r f^{(r)}(b) + \sum_{i=0}^{r-1} c'_i b^i f^{(i)}(b).$$

Q. E. D.

---

[3] From this lemma it is possible to obtain an identity given on page 20 of Boole's "Finite differences." For if $f(b)$ is of the n-th degree and b_1 is a root of multiplicity n, then

$$f(b) = a_0 \sum_{i=0}^{n} (-1)^{n-i} \frac{n(n-1)\cdots(n-1+i)}{i!} b^i b_1^{n-i}$$

$$f(b_1) = f'(b_0) = \cdots = f^{(n-1)}(b_1) = 0 \quad\text{and}\quad f^{(n)}(b_1) = a_0 n!\,.$$

Now from the lemma

$$b_1^n f(n)(b_1) = a_0 \sum_{i=0}^{n} (-1)^{n-i} \frac{i^n n(n-1)\cdots(n-i+1)}{i!} b_1^i b_1^{n-i}.$$

$$\therefore \qquad a_0 b_1^n n! = a_c b_1^n \sum_{i=0}^{n} (-1)^{n-i} \frac{i^n n(n-1)\cdots(n-i+1)}{i!}.$$

Hence,

$$(n-1)! = n^{n-1} - (n-1)^n + \frac{(n-1)(n-2)^n}{2!} - \frac{(n-1)(n-2)(n-3)^n}{3!} + \cdots \pm (n-1)2^{n-1} \pm 1.$$

If Adams had utilized this he would have simplified his results concerning irregular linear difference equations for the case where all roots of the characteristic equation are equal. See C. R. Adams, "On the irregular cases of the linear ordinary difference equation," *Transactions of the American Mathematical Society*, vol. 30 (1928), p. 526. See also G. D. Birkhoff and W. J. Trjitzinsky, "Analytic theory of singular difference equations," *Acta Mathematica*, vol. 60, pp. 1-89.

Hence the statement holds for r.

When the coefficients of $x^{-(j/\omega h)}$ $(j=1,2,\cdots,\omega-1)$ in (19) are set equal to zero, we obtain equations which are satisfied for all values of $\delta_1,\delta_2,\cdots,\delta_{\omega-1},\ s_0,s_1,\cdots,s_{\omega-1}$. For, these relations are composed of polynomials in these constants whose coefficients vanish, since they are (after the lemma) of the form $\sum_{i=0}^{\omega-1} c_i b^i f^{(i)}(b_1)$.

Placing the coefficient of $x^{-(1/h)}$ equal to zero, and employing the relation (20), we have

$$\delta_1{}^\omega \frac{(h\omega-1)^\omega b_1{}^\omega f^{(\omega)}(b_1)}{\omega!(\omega h)^\omega}=-\phi_1(a,b_1).$$

And since by hypothesis b_1 is not a root of $\phi_1(a,b_1)=0$ this equation determines ω distinct values for δ_1.

When the coefficients of $x^{-[(\omega+j)/\omega h]}$ $(j=1,2,\cdots)$ are equated to zero, we have

$$\delta_{j+1}\frac{(\omega h-j)(h\omega-1)^{\omega-1}b_1{}^{(\omega)}f^{(\omega)}(b_1)\delta_1{}^{\omega-1}}{(\omega-1)!\,(\omega h)^\omega}=\psi_j(\delta_1,\cdots,\delta_j,a,b_1)$$
$$(j=1,2,\cdots,\omega h-2),$$
$$d\,\frac{(\omega h-1)^{\omega-1}b_1{}^\omega f^{(\omega)}(b_1)\delta_1{}^{\omega-1}}{(\omega h)^{\omega-1}(\omega-1)!}=\psi_{\omega h-1}(\delta_1,\cdots,{}_{\omega h-1},a,b_1)$$
$$\frac{(j-\omega h+1)(\omega h-1)^{\omega-1}\delta_1{}^{\omega-1}b_1{}^\omega f^{(\omega)}(b_1)}{(\omega h)^\omega(\omega-1)!}s_0{}^q s_{j-\omega h+1}=\psi_j(\delta_1,\cdots,\delta_j,a,b_1)$$
$$(j=\omega h,\omega h+1,\cdots),$$

where the expressions ψ_j are polynomials in the previously determined constants. Hence, for each of the ω values of δ_1 there is one and only one value for each of the constants $\delta_2,\delta_3,\cdots,\delta_{\omega h-1},\ d,\ s_1/s_0,\ s_2/s_0,\cdots$.

The solutions are all linearly independent, therefore:

THEOREM 7. *A homogeneous algebraic difference equation has ν and only ν linearly independent formal solutions of the form* (2), *where ν is the difference between the maximum and the minimum values of $i_1+i_2+\cdots+i_q$, if the multiple roots of the characteristic equations are not roots of the corresponding secondary equations and if the Puiseux diagram does not have any multiple point vertices for which* $\sum_{i_1+i_2+\ldots+i_q=\varpi r} a'_{0i_1i_2\ldots i_q}=0$.

COROLLARY 7. 1. *A homogeneous algebraic difference equation of the m-th order and the q-th degree, which contains both the terms $c_1(x)[y(x+m)]^q$ and $c_2(x)[y(x)]^q$, $c_1(x)c_2(x)\not\equiv 0$, has mq and only mq linearly independent solutions of the form* (2) *if the multiple roots of the characteristic equations*

are not roots of the corresponding secondary equations and if the Puiseux diagram does not have any multiple point vertices for which

$$\sum_{i_1+i_2+\cdots+i_q=xr} a'_{0i_1i_2\ldots i_q}=0.$$

Now let us view briefly a few cases in which a multiple root of a characteristic equation is also a root of the secondary equation.[4]

If a characteristic equation has a root b_1 of multiplicity $\omega>2$ which is a simple root of the corresponding secondary equation, and if $a=c/h$, where $h>1$, then there exist formal solutions: One of the form

$$(21)\quad \begin{cases} (\mathrm{a})\ \ y(x)=b_1^x x^{ax} x^d e^{L^{(h)}(x)}\cdot R(x^{-[1/h(\omega-1)]}) \\ \qquad\qquad \text{and } \omega-1 \text{ of the form} \\ (\mathrm{b})\ \ y(x)=b_1^x x^{ax} x^d e^{L^{[h(\omega-1)]}(x)} R(x^{-[1/h(\omega-1)]}). \end{cases}$$

When $h=1$ the ω formal solution (21) exist if

$$b_1\phi_1(b_1) -\frac{1}{2!\,(\omega-1)}\sum_{i_1=0,\,i_2=0,\ldots,\,i_q=0}^{m}(i_1^2+i_2^2+\cdots+i_q^2)a''_{0i_1i_2\ldots i_q}(be^a)^{i_1i_2+\cdots+i_q}\neq 0$$

and

$$(22)\quad \frac{(\omega-2)^{\omega-1}\delta_1^{\omega-1}b_1^{\omega}f^{(\omega)}(b_1)}{(\omega-1)!\,(\omega-1)^{\omega-1}}+b_1\phi_1(b_1)-\frac{j}{(\omega-1)\cdot 2!} \times\sum_{i_1=0,\,i_2=0,\ldots,\,i_q=0}^{m}(i_1^2+i_2^2+\cdots+i_q^2)a''_{0i_1i_2\ldots i_q}(be^a)^{i_1+i_2+\cdots+i_q}\neq 0$$

for $j=2,3,4,\cdots$. In particular, the two conditions are satisfied for all m values of δ_1 if

$$\sum_{i_1=0,\,i_2=0,\ldots,\,i_q=0}^{m}(i_1^2+i_2^2+\cdots+i_q^2)a'_{0i_1i_2\ldots i_q}b^{i_1+i_2\cdots+i_q}e^{a(i_1+i_2\cdots+i_q)}=0.$$

When $\omega=2$, the solutions (21) both reduce to the type (a), but, in order for the equation to possess two solutions of this type, further conditions must be fulfilled.

When b_1 is a ω-fold root of the characteristic equation and is a multiple root of the secondary equation the problem is more complicated. We cannot state as Adams[4] did for the case of the linear homogeneous difference equations, "that the presence of b_1 as a ω_1-fold root of the secondary equation tends to reduce to $\omega-\omega_1$ the index of the root of x^{-1} according to powers of which the series proceed." For such a statement cannot hold unless

[4] C. R. Adams has treated the irregular cases of the linear difference equation. *Transactions of the American Mathematical Society*, vol. 30 (1928), pp. 507-541.

$$\sum_{i_1=0,\, i_2=0,\dots,\, i_q=0}^{m} (i_1^2 + i_2^2 + \cdots + i_q^2) a''_{0 i_1 i_2 \dots i_q} (be^a)^{i_1+i_2 \cdots + i_q} = 0$$

and even then, for ω sufficiently large other conditions must also be satisfied.

If $\omega \leq h$ and b_1 is a root of multiplicity $\geq \omega$ of $\phi_1(b_1, a) = 0$, a root of multiplicity $\geq \omega - 1$ of $\phi_2(b_1, a) = 0, \cdots$, a root of multiplicity ≥ 2 of $\phi_{\omega-1}(b_1, a) = 0$, and is not a root of $\phi_\omega(b_1, a) = 0$, then there are ω formal solutions of the type

$$y(x) = b_1^x x^{ax} x^d e^{L^{(h)}(x)} \cdot R(x^{-(1/h)}).$$

If b_1 is a root of all $\phi_i(b_1, a) = 0$ $(i = 1, 2, \cdots)$ then there is a solution of the form $y(x) = b_1^x$. If $\omega > h$ again the problem has additional complications. The equations for the determination of the coefficients $\delta_1, \delta_2, \cdots, \delta_{p-1}$, $d, s_1/s_0, s_2/s_0, \cdots$ contain terms whose coefficients are of the form

$$\sum_{i_1=0,\, i_2=0,\dots,\, i_q=0}^{m} (i_1^l + i_2^l + \cdots + i_q^l) b^{i_1+i_2+\cdots+i_q} e^{a(i_1+i_2+\cdots+i_q)} a''_{j i_1 i_2 \dots i_q},$$

$(l = 2, 3, \cdots, K,\ j = 0, 1, 2, \cdots, K)$, and

$$\sum_{i_1=0,\, i_2=0,\dots,\, i_q=0}^{m} \ \sum_{j_1, j_2, \dots, j_l}^{q} i_{j_1} i_{j_2} \cdots i_{j_l} (be^a)^{i_1+i_2+\cdots+i_q} a''_{j i_1 i_2 \dots i_q},$$

$$(l \leqq 2, 3, \cdots, j = 0, 1, 2, \cdots).$$

Such quantities cannot be expressed as a linear combination of the various derivatives of the characteristic, secondary, $\cdots$ equations, hence, we cannot, on the basis of the multiplicity of the root b of these equations, determine when the coefficient of the undetermined quantities are non-vanishing.

5. Equations with an infinite number of solutions. In the above considerations, we have found that homogeneous difference equations which satisfy certain restrictive conditions have only a finite number of formal solutions of the type (2). However, there are, as is evidenced by the following obvious theorem, difference equations which have an infinite number of solutions of the form (2).

THEOREM 8. *If $i_1 + i_2 + \cdots + i_q = K$ for all terms of a non-linear homogeneous algebraic difference equation and if the sum of all the coefficients vanish identically in x, then there are an infinite number of solutions* (2). [$y(x) = b_1^x$ is a solution for all values of b_1].

Theorem 8 applies to a special class of difference equations whose Puiseux diagrams have multiple point vertices for which $\sum_{i_1+i_2+\cdots+i_q=x_r} a'_{0 i_1 i_2 \dots i_q} = 0$. Before considering the family of all such equations, let us see whether the difference equations whose Puiseux diagrams do not have multiple point vertices for which $\sum_{i_1+i_2+\cdots+i_q=x_r} a'_{0 i_1 \dots i_q} = 0$ may have an infinite number of

solutions (2). For each difference equation of this class the values of a and b are uniquely determined and are finite in number, hence, if there are an infinite number of solutions (2) there must be an infinite number of values for someone of the quantities δ_i $(i=1,2,\cdots,p-1)$, d or s_i/s_0 $(i=1,2,\cdots)$. It is possible for one of these quantities to have an infinite number of values. For example: the expressions (22) give the coefficients of the constants $\delta_i, d, s_i/s_0$ in the linear equations which determine them. Hence if (22) vanish for some j, say $j=2$, and the other term of the equation for the determination of δ_2 also vanishes, then δ_2 is arbitrary, while all the other constants $\delta_i, d, s_i/s_0$ are uniquely determined since (22) can vanish for only one value of j.

It is conceivable that the equations for the determination of the constants $\delta_i, d, s_i/s_0$ may all have a degree greater than unity. If this were the case the difference equation might be satisfied by each series of a "branched set of series" infinite in number. For example, if all the equations for the determination of the constants are of the second degree and the roots of all the equations are distinct, then there would be $2^{l+\omega}$ values for s_l/s_0. Hence there would be a countable infinity of solutions of the form (2). Such a condition can never actually exist, as can be seen by inspecting the supposed identity. For when the degree of the equation for the determination of d is $M>1$, the degree of the equation for the determination of s_1/s_0 is $M_1<M$, the degree of the equation for the determination of s_2/s_0 is $M_2 \leqq M_1$, (the equality sign only holds when $M_1=1$), and so on, until the degree of the equation for determining the constant s_r/s_0 is one.

Returning to the study of the class of difference equations whose Puiseux diagrams have multiple point vertices for which $\sum\limits_{i_1+i_2+\cdots+i_q=x_r} a'_{0i_1i_2\cdots i_q}=0$, we first consider homogeneous difference equations which have the property that $i_1+i_2+\cdots+i_q=K$ for all terms, i. e.,

$$(23)\quad \sum_{i_1+i_2+\cdots+i_q=K}\left(a_{0i_1\cdots i_q}+\frac{a_{1i_1\cdots i_q}}{x}+\cdots\right) \times y(x+i_1)y(x+i_2)\cdots y(x+i_q)=0.$$

Here it is not possible to obtain solutions which proceed by fractional powers of x, so we look for solutions of the form

$$(24)\qquad y(x)=x^{ax}b^x x^d(s_0+s_1/x+s_2/x^2+\cdots).$$

The substitution of this expression in (23) gives

$$(25)\quad \sum_{i_1+i_2+\cdots+i_q=K}\left(a_{0i_1i_2\cdots i_q}+\frac{a_{1i_1i_2\cdots i_q}}{x}+\frac{a_{2i_1\cdots i_q}}{x^2}+\cdots\right) \cdot A(x)\cdot D(x)\cdot S(x,1)=0.$$

Equating the coefficients of the powers of $1/x$ to zero, we have

$$\frac{a}{2}\Sigma\,(i_1^2+i_2^2+\cdots+i_q^2)a_{0i_1i_2\ldots i_q}+\Sigma\,a_{1i_1\ldots i_q}=0$$

$$-\frac{d}{2}\Sigma\,(i_1^2+i_2^2+\cdots+i_q^2)a_{0i_1\ldots i_q}+P_0(a,a_{ji_1\ldots i_q})=0$$

$$\frac{l(l+1)}{2!}\frac{s_l}{s_0}\Sigma\,(i_1^2+i_2^2+\cdots+i_q^2)a_{0i_1\ldots i_q}$$
$$+P_l\left(a,d,a_{ji_1\ldots i_q},\frac{s_1}{s_0},\cdots,\frac{s_{l-1}}{s_0}\right)=0,$$
$$(l=1,2,3,\cdots),$$

where the expressions P_l involve only previously determined constants. Hence, if

$$(26)\qquad \Sigma\,(i_1^2+i_2^2+\cdots+i_q^2)a_{0i_1i_2\ldots i_q}\neq 0$$

there are always an infinite number of formal solutions of the form (24),—one for each non-zero value of b. When the inequality (26) is not satisfied, there are no solutions of the desired type unless

$$(27)\qquad \Sigma\,a_{1i_1i_2\ldots i_q}=0.$$

If the equality (27) holds and the inequality (26) does not, then the equations which determine the constants are

$$(28)\quad \frac{a^2}{8}\Sigma\,(i_1^2+i_2^2+\cdots+i_q^2)^2a_{0i_1i_2\ldots i_q}+\frac{a}{2}\Sigma\,[(i_1^2+\cdots+i_q^2)a_{1i_1i_2\ldots i_q}$$
$$-\tfrac{1}{3}(i_1^3+\cdots+i_q^3)a_{0i_1\ldots i_q}]+\Sigma\,a_{2i_1\ldots i_q}=0$$

$$d^2Q_0-d\,\Sigma\,[(i_1^2+\cdots+i_q^2)\{a_{1i_1\ldots i_q}+\frac{a}{2}(i_1^2+\cdots+i_q^2)a_{0i_1\ldots i_q}\}$$
$$-\tfrac{2}{3}(i_1^3+\cdots+i_q^3)a_{0i_1\ldots i_q}]+P_{01}=0$$

$$(29)\quad \left(\frac{s_l}{s_l}\right)^2Q-\frac{s_l}{s_0}\frac{l(l+1)}{2!}\Sigma\,[(i_1^2+\cdots+i_q^2)\{a_{1i_1\ldots i_q}$$
$$+\frac{a}{2}(i_1^2+\cdots+i_q^2)a_{0i_1\ldots i_q}\}-\frac{l+2}{3}(i_1^3+\cdots+i_q^3)a_{0i_1\ldots i_q}]+P_{0l}=0,$$

$(l=1,2,3,\cdots)$, where Q_i and P_{0i} $(i=-1,0,1,2,\cdots)$ are known quantities. When

$$(30)\quad \Sigma\,[(i_1^2+i_2^2+\cdots+i_q^2)a_{1i_1\ldots i_q}-\tfrac{1}{3}(i_1^3+\cdots+i_q^3)a_{0i_1\ldots i_q}]\neq 0$$

there is at least one value for a. And when a is a root of (28) such that

$$(31)\quad \Sigma\,[(i_1^2+\cdots+i_q^2)\{a_{1i_1\ldots i_q}+\frac{a}{2}(i_1^2+\cdots+i_q^2)a_{0i_1\ldots i_q}\}$$
$$-\frac{l+2}{3}(i_1^3+\cdots+i_q^3)a_{0i_1\ldots i_q}]\neq 0$$

for $l=0,1,2,\cdots$, then it is possible to determine at least one value for each of the constants d and s_l/s_0, since the coefficients of the linear terms in the

equation (29) do not vanish. Hence, there is always at least one formal solution for each value of b. When the inequality (30) holds and

$$\Sigma\, a_{2i_1i_2\ldots i_q}=0,$$

then the condition (31) may be replaced by

$$(31')\quad \Sigma\left[(i_1^2+\cdots+i_q^2)a_{1i_1\ldots i_q}-\frac{l+2}{3}(i_1^3+\cdots+i_q^3)a_{0i_1\ldots i_q}\right]\neq 0,$$

for $l=0,1,2,\cdots$, since a may be zero.

In the general case the coefficients of the powers of $1/x$ up to and including $(1/x)^{n-2}$ vanish identically for all values of the unknowns. This is the case when

$$(32)\quad \Sigma\,(i_1^{j_1}+i_2^{j_1}+\cdots+i_q^{j_1})(i_1^{j_2}\cdots+i_q^{j_2})\cdots\cdots(i_1^{j_t}+\cdots+i_q^{j_t})a_{li_1\ldots i_q}=0,$$

where $l\leq n-1$, $j_1\geq j_2\geq\cdots\geq j_t$, $j_1+j_2+\cdots+j_t\leq n-1-l$. If the equalities (32) hold and if

$$(33)\quad \sum_{j=2}^{n}\ \sum_{i_1+i_2+\ldots+i_q=K}(-1)^j\frac{(\gamma+j-1)(\gamma+j-2)\cdots(\gamma+2)}{j!}\times(i_1^j+\cdots+i_q^j)a_{(n-j)i_1\ldots i_q}\neq 0$$

for $\gamma=-1,0,1,2,\cdots$, then the coefficient of $(1/x)^{n-1}$ is an algebraic equation in a which does not contain any of the other undetermined constants. Moreover, the constant term in this equation is zero and the coefficient of the linear term is different from zero [(33) for $\gamma=-1$]. Hence $a=0$ is a solution. The coefficient of $(1/x)^n$ gives an equation for the determination of d, the coefficient of $(1/x)^{n+1}$ gives an equation for the determination of $s_1/s_0,\cdots$, and in each of these equations the coefficient of the linear term is different from zero. Therefore, the constants d, s_γ/s_0 may be determined in order.[5]

Hence:

---

[5] In order to see the validity of the above statement it is convenient to write

$$(1+i_1/x)^d(1+i_2/x)^d\cdots(1+i_q/x)^d=\exp\{d[\log(1+i_1/x)+\log(1+i_2/x)+\cdots+\log(1+i_q/x)]\}$$
$$=\exp\left\{d\left[\frac{i_1+i_2+\cdots+i_q}{x}-\frac{i_1^2+\cdots+i_q^2}{2x^2}+\frac{i_1^3+i_2^3+\cdots+i_q^3}{3x^3}\cdots\right]\right\}$$
$$=1+\frac{d(i_1+i_2+\cdots+i_q)}{x}-\frac{(i_1^2+i_2^2+\cdots+i_q^2)d-2(i_1+\cdots+i_q)^2d^2}{x^2}+\frac{\cdots}{x^3}+\cdots$$

Since in this formal expression the coefficients of the powers of $1/x$ are polynomials in d with coefficients of the form

$$(i_1^{j_1}+\cdots+i_q^{j_1})(i_1^{j_2}+\cdots+i_q^{j_2})\cdots(i_1^{j_t}+\cdots+i_q^{j_t}).$$

THEOREM 9. *A non-linear algebraic homogeneous difference equation, in which $i_1 + i_2 + \cdots + i_q = K$ for all terms, has an infinite number of formal solutions of the form* (24) *if the relations* (32) *and* (33) *are satisfied.*

The conditions of this theorem are more restrictive than necessary. A more general statement is the following: If the relations (32) hold for $l \leq n - 2$; if

$$\sum_{j=2}^{n} \sum_{i_1 + \cdots + i_q = K} (-1)^j \frac{1}{j(j-1)} (i_1{}^j + i_2{}^j + \cdots + i_q{}^j) a_{(n-j) i_1 \ldots i_q} \neq 0,$$

and if there exists an a (defined by setting the coefficient of $(1/x)^{n-1}$ equal to zero) such that

$$\sum_{j=2}^{n} \sum_{i_1 + i_2 + \cdots + i_q = K} (-1)^j \frac{(\gamma + j - 1)(\gamma + j - 2) \cdots (\gamma + 2)}{j!} \times (i_1{}^j + \cdots + i_q{}^j) a_{(n-j) i_1 i_2 \ldots i_q} \neq 0$$

for $\gamma = 0, 1, 2, \cdots$, then (23) has an infinite number of solutions of the form (24). Although this statement is still very restrictive, because of the algebraic complications we have not attempted to obtain better results.

We now treat the general case.

Here there are an infinite number of rational values for a such that the terms corresponding to some multiple point vertex are of higher degree than any other term of the equation. For $a = c/h$ we assume a solution of the form (2), where $p = h$. When y is replaced by this value and the common factor removed the supposed identity is

$$(34) \quad \sum_{i_1 = 0,\, i_2 = 0, \ldots,\, i_q = 0}^{m} \left(a''_{0 i_1 \ldots i_q} + \frac{a''_{1 i_1 \ldots i_q}}{x^{1/h}} + \cdots \right) (be^a)^{i_1 + i_2 + \cdots + i_q} \cdot D(x) \cdot \Delta_1(x, h) \cdot \Delta_2(x, h) \cdots \Delta_{h-1}(x, h) \cdot S(x, h) \equiv 0.$$

If the coefficients of the powers of $1/x^{1/h}$ equal zero, then b is determined by the equation

$$(35) \qquad \psi_1(b) = \sum_{i_1 = 0,\, i_2 = 0, \ldots,\, i_q = 0}^{m} a''_{1 i_1 \ldots i_q} (be^a)^{i_1 + i_2 + \cdots + i_q} = 0.$$

The coefficients of the linear terms in the linear equations which determine δ_j, $(j = 1, \cdots, p - 1)$, d and s_j/s_0 $(j = 1, 2, \cdots)$ are of the form $M_i b \psi'_1(b)$, $(M_i \neq 0)$. Hence, if (35) has a simple non-zero root there is a formal solution (2). Therefore, there are in infinite number of formal solutions if there are an infinite number of values a for which the corresponding equations (35) have a simple non-zero root.

We state that there can never be an infinite number of rational values of a for which the corresponding equations (35) have a simple non-zero root.

Construct the Puiseux diagram including a point for each term of the given difference equation. (See Figure 3.) If l is a line through the multiple point vertex P with a slope $-a$, then the equation for the determination of b has for its coefficients the coefficients of the terms corresponding to points lying in some line l' which is parallel to l. If the equation (35) is to have a simple non-zero root the line l' must pass through at least two distinct points. But since the number of points in the diagram are finite (the coefficients of the equations are polynomials) the number of possible lines connecting two distinct points is finite. Hence our statement is true.

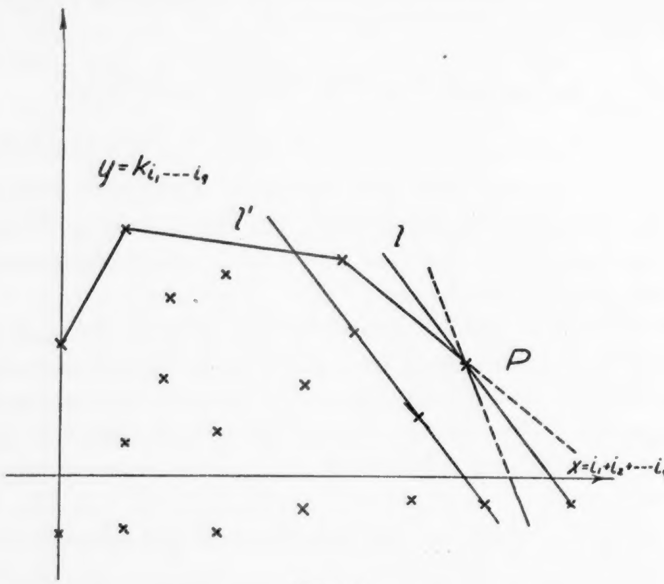


FIG. 3.

When equation (35) vanishes identically, b is determined by the first one of the equations,

$$(36)\quad \psi_{1j}(b) = \sum_{i_1=0,\, i_2=0, \ldots,\, i_q=0}^{m} a''_{ji_1 \ldots i_q}(be^a)^{i_1+i_2+\cdots+i_q} = 0 \quad (j = 2, 3, \cdots, h),$$

which is not an identity. In case any one of them has a simple non-zero root then the other constants are all uniquely determined. If equations (36) $j = 1, 2, 3, \cdots, h$ are identities for all values b and if

$$(37)\qquad \sum_{i_1=0,\, i_2=0, \ldots,\, i_q=0}^{m} (i_1^2 + i_2^2 + \cdots + i_q^2)a'_{0i_1 \ldots i_q} \neq 0,$$

then the constants δ_j, d and s_j/s_0 are determined for every value of b. Hence there are an infinite number of solutions. It is easy to see further that if

there exists an a such that the equations (36) are identities in b for $j=0,1,2,\cdots,h+\lambda$ where λ is the first value of $\lambda<h$ for which

$$(38)\qquad \sum_{i_1=0,\,i_2=0,\ldots,\,i_q=0}^{m} a_{s_1 i_1\ldots i_q}(i_1^2+\cdots+i_q^2)(be^a)^{i_1+i_2+\cdots+i_q}\neq 0,$$

then again the constants are determined for an infinite number of b's. For if (38) is satisfied for one value of b it is satisfied by an infinite number of values. When no a exists such that (38) holds for $\lambda<h$ but there exists an a such that (36) holds for $j=0,1,2,\cdots,\lambda+h$; $h\leqq\lambda<2h$, where λ is the first value for which

$$\sum_{i_1=0,\,i_2=0,\ldots,\,i_q=0}^{m}\Big[(i_1^2+\cdots+i_q^2)a''_{3i_1\ldots i_q} - \left(\frac{2h+\gamma}{3h}\right)(i_1^3+i_2^3+\cdots+i_q^3)a_{\lambda-hi_1\ldots i_q}\Big](be^a)^{i_1+i_2+\cdots+i_q}=0$$

$\gamma=-h+1,-h+2,\cdots,-1,0,1,\cdots$ then, again the constants may be determined for an infinite number of solutions.

In general, when there exists an a such that

$$(39)\qquad \sum_{i_1=0,\,i_2=0,\ldots,\,i_q=0}^{m}(i_1^{j_1}+i_2^{j_1}+\cdots+i_q^{j_1})(i_1^{j_2}+i_2^{j_2}+\cdots+i_q^{j_2})\cdots\cdot (i_1^{j_t}+\cdots+i_q^{j_t})a''_{li_1i_2\ldots i_q}(e^ab)^{i_1+i_2+\cdots+i_q}\equiv 0$$

for all positive integers such that $(j_1+j_2+\cdots+j_t-t)h+t\leqq nh+k-l$ the coefficients of $1/x^\alpha$ $(\alpha=0,1/h,2/h,\cdots,n+k/h)$ vanish for all values of the constants $\delta_1,\delta_2,\cdots,\delta_{h-1}$, d, s_1/s_0, $s_2/s_0,\cdots$. If the identities (39) are satisfied and if there exists a b such that

$$(40)\qquad \sum_{j=2}^{n+1}\ \sum_{i_1=0,\,i_2=0,\ldots,\,i_q=0}^{m}(-1)^j\left(\frac{1}{h}\right)\left(\frac{h+\gamma}{2h}\right)\cdots\left(\frac{[j-1]h+\gamma}{jh}\right) \times(i_1^j+i_2^j+\cdots+i_q^j)a''_{[(n+1-j)h+k]i_1i_2\ldots i_q}(be^a)^{i_1+\cdots+i_q}\neq 0$$

$\gamma=-h+1,-h+2,\cdots,-1,0,1,\cdots$, then the coefficients of the linear terms in the equations which determine the constants δ_i, d, s_j/s_0 are of the form (40). Therefore, the quantities δ_i, d, s_j/s_0 may be determined in the order of their sequence. When the inequalities (40) hold for one value of b, they hold for an infinite number of values. Hence we have the following theorem:

THEOREM 10. *A non-linear homogeneous algebraic difference equation, whose Puiseux diagram has a multiple point vertex at* $x=x_r$ *for which* $\sum_{i_1+i_2+\ldots+i_q=x_r} a'_{0i_1\ldots i_q}=0$, *has an infinite number of formal solutions of the form* (2) *if for an admissible* a *there exists a* b *such that the relations* (39) *and* (40) *are satisfied.*

Theorems 8 and 9 are special cases of Theorem 10.

Case II. The series (2) *does not cause each of the homogeneous parts to vanish.*

It follows from Theorem 1 that a formal solution (2) which does not cause each of the homogeneous parts to vanish must be one in which $a=0$, $\delta_i=0$ $(i=1,\cdots,p-1)$ and $b=1$, i.e.,

$$y(x)=x^d R(x^{-(1/p)}). \tag{41}$$

When (41) is a formal solution of the general algebraic difference equation

$$\sum_{j=0}^{q}\sum_{i_1=0,\ldots,i_q=0}^{m} x^{k_{ji_1i_2\cdots i_q}}\left(a_{0i_1i_2\ldots i_j}+\frac{a_{1i_1\ldots i_j}}{x}+\cdots\right)$$
$$\times\, y(x+i_1)y(x+i_2)\cdots y(x+i_j)=0,$$

then

$$\sum_{j=0}^{q}\sum_{i_1=0,\ldots,i_q=0}^{m} x^{k_{ji_1}\cdots i_q+dj}\left(a_{0i_1i_2\ldots i_j}+\frac{a_{1i_1\ldots i_j}}{x}+\cdots\right)$$
$$\times\, R((x+i_1)^{-(1/p)})R((x+i_2)^{-(1/p)})\cdot\cdots\cdot R((1+i_j)^{-(1/p)})\equiv 0.$$

If this relation is an identity in x, two of the leading terms must be of the same degree. While all other terms are of lower degree. That is, d must be determined so that

$$k_{j_1i_1\ldots i_{j_1}}+j_1d=k_{j_2i_1\ldots i_{j_2}}+j_2d$$

where the values $j_1, i_1,\cdots,i_{j_1}$ are not all equal to the values $j_2, i_1,\cdots,i_{j_2}$ respectively, and where

$$k_{ji_1i_2\ldots i_j}+jd\leq k_{j_1i_1\ldots i_{j_1}}+j_1d$$

for all other values of $j, i_1,\cdots,i_j$. Here again these conditions may be represented by a Puiseux diagram. For if we plot the points $(j, k_{ji_1\ldots i_j})$, (See Figure 4) the negatives of the slopes of the lines connecting two such points give all conceivable values for d. Hence we are led to a broken line, L, concave downward, whose vertices fall at certain of these points while all other points lie below L. Again, it is possible for two points or more to coincide at a vertex of the diagram. When L has a multiple point vertex for which $\sum_{j_r} a'_{0i_1\ldots i_{j_r}}=0$, any value of an interval is an admissible value for d, but when L does not have double point vertices the slopes of the segments of L uniquely determine the values of d.

Under the assumption that the Puiseux diagram does not have any multiple point vertices for which $\sum_{j_r} a'_{0i_1\ldots i_{j_r}}=0$, d has n rational values. For each of these values there is a corresponding equation

(42) $$\psi_{d_i}(s_0) = 0$$

which determines the values for s_0. If we denote the n values by $d_1, d_2, \cdots, d_n$, where $d_1 > d_2 > \cdots > d_n$, then the total number of non-zero values for s_0 (counting the roots according to their multiplicity in the various equations) is *precisely* q. For if $j_0, j_1, \cdots, j_n$ are the values of the successive vertices the number of roots of the n equations corresponding to $d_1, d_2, \cdots, d_n$ are $j_1 - j_0, j_2, \cdots, j_n - j_{n-1}$, respectively.

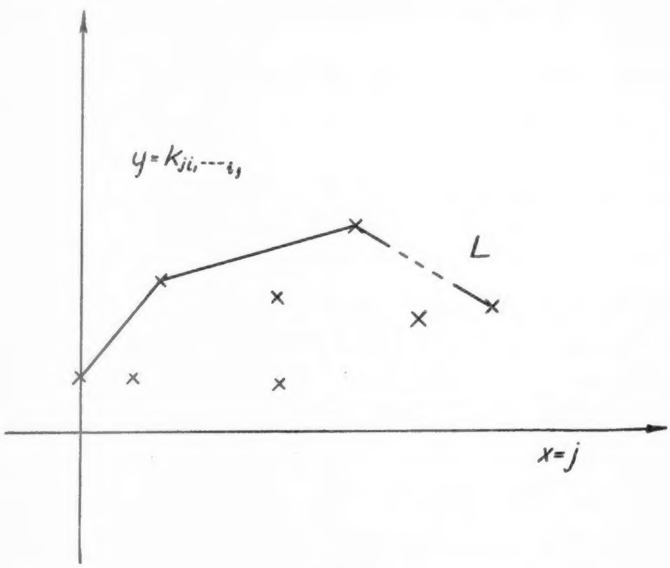


FIG. 4.

For a rational value $d_i = c/h$ it is necessary to set p equal to h in order to insure that the coefficients of the powers of $(1/x)^{1/p}$ contain at least one undetermined contsant s_l. The products

$$R((x+i_1)^{-(1/h)}) \cdot R((x+i_2)^{-(1/h)}) \cdot \cdots \cdot R((x+i_j)^{-(1/h)})$$

are of the form

$$\cdots \quad s_0^j + \frac{js_1s_0^{j-1}}{x^{1/h}} + \frac{js_2s_0^{j-1} + \text{terms involving } s_0 \text{ and } s_1}{x^{2/h}} + \cdots.$$

Therefore, the coefficients of the constants s_i in the linear equations which determine them are $\psi'_{d_i}(s_0)$. Hence, *if the equations* (42) *do not have multiple roots there are always q solutions of the form* (41).

THE UNIVERSITY OF MARYLAND,
COLLEGE PARK, MD.

CONCERNING THE CONVEXIFICATION OF CONTINUOUS CURVES.*

By Orville G. Harrold, Jr.

1. It is the purpose of this paper to show that certain classes of bounded continuous curves can be regarded as convex spaces on the introduction of an appropriate metric.

By a metric space is meant a set of points for which a non-negative real number ρ is defined for each pair of points in the set satisfying the usual conditions

1. $\rho(a,b)=0$ if and only if $a=b$,
2. $\rho(a,b)=\rho(b,a)>0, \quad a\neq b$,
3. $\rho(a,b)+\rho(b,c)\geqq\rho(a,c)$.

The distance function ρ is called a metric of the space. The point b will be called a between point of a and c (and of c and a) if and only if it is distinct from each of a and c and further $\rho(a,b)+\rho(b,c)=\rho(a,c)$. A metric space R will be called convex (Menger [1]) if to every pair of distinct points x, y in R at least one between point exists. A topological or metrical space is called convexifiable if it is homeomorphic with a convex metric space.

2. Menger [2] has shown that every compact im kleinen connected continuum which is arc lengthwise im kleinen connected [3] may be convexified by re-defining the distance function in an appropriate way. The question arises as to whether or not it is possible for every continuous curve to define the metric in such a way that the curve is arc lengthwise im kleinen connected and hence convexifiable. It can be shown, for instance, that it is not possible to define a metric throughout the interior and on the boundary of a Jordan region in such a way that for all curves imbedded in this region the property of arc lengthwise connectedness im kleinen exists. It appears that the choice of a metric by means of which the curve, which may be regarded as the space,

* Received April 28, 1937; Revised July 6, 1938.

[1] K. Menger, "Untersuchungen über allgemeine Metrik," *Mathematische Annalen*, Bd. 100, pp. 75-163.

[2] K. Menger, *loc. cit.*

[3] The set M is said to be arc lengthwise im kleinen connected provided that to every $\epsilon>0$ there exists a $\delta>0$ such that $\rho(p,q)<\delta$ implies that p and q can be joined by an arc in M of length less than ϵ.

is to be convexified will depend largely on the structure of the curve with which we are dealing.

It has been shown by Kuratowski and Whyburn [4] that acyclic curves can be convexified, and further, that this property of a continuum is cyclicly extensible, hence in all cases it will suffice to limit our considerations to the true cyclic elements of the various curves. The point p of M is called an im kleinen cycle point of M if for each $\epsilon > 0$, p lies on some simple closed curve in M of diameter $< \epsilon$. It will be shown that the following types of curves [5] are convexifiable:

a) plane continuous curves having at most a finite number of complementary domains,

b) bestandig regular curves, and

c) curves having a set of im kleinen cycle points K such that $\bar{K}$ is totally disconnected.

3. The proof of 2. a) for the case of a single complementary domain is immediate since each true cyclic element (in case the curve M is not acyclic) is topologically equivalent to a closed unit circle.

In case M has two complementary domanis R_1, R_2 we distinguish according as $C = B(R_1)B(R_2)$ [6] $= 0$, or $\neq 0$. In the first case M is homeomorphic to the closed circular ring [7] $1 \leqq r \leqq 2$, $0 \leqq \phi \leqq 2\pi$ which is clearly arc lengthwise im kleinen connected. If $C \neq 0$, two cases are distinguished according as $B(R_1) = B(R_2)$ or $B(R_1) \neq B(R_2)$. If the first relation holds, M is a topological circle and can be convexified. In the second case let the at most countable number of components of $B(R_2) - B(R_2)B(R_1)$ be $t_1, t_2, t_3, \cdots$. Each $\bar{t}_i$ will be an arc with end-points a_i, b_i in $B(R_1)$, except in case $B(R_2) - B(R_2)B(R_1)$ has a single component $\bar{t}_1$ may be $B(R_2)$ itself. To each t_i corresponds an unique closed Jordan region $\bar{D}_i$ contained entirely in M such that t_i plus an arc s_i of $B(R_1)$ forms the boundary of $\bar{D}_i$. Every point of M is contained in $B(R_1) + \sum_1^\infty \bar{D}_i$, hence $M = B(R_1) + \sum_1^\infty \bar{D}_i$. Map the interval $0 \leqq t \leqq 1$ on $B(R_1)$ so that $t = 0$, $t = 1$ correspond to a point $q \in B(R_1)B(R_2)$. To the unique arc a_ib_i of $B(R_1)$ not passing through q will

[4] Kuratowski et Whyburn, "Sur les elements cycliques et leurs applicatione," *Fundamenta Mathematicae*, Tome 16, pp. 305-331.

[5] Unless stated otherwise it is understood that all curves mentioned lie in a Euclidean space of n dimensions.

[6] $B(R)$ denotes the boundary of the region R.

[7] B. V. Kerekjarto, *Topologie 1*, II, 2.

correspond an interval e_i of $0 \leqq t \leqq 1$. On e_i construct an equilateral triangle with e_i as base. Denote the triangle plus its interior by g_i, then g_i can be mapped topologically on $\bar{D}_i$ with $a_i b_i$ corresponding to e_i. Call the point-set thus constructed on the unit interval N, and let T denote the above described transformation which carries N into M. Evidently T is one-valued and continuous on N and each point in M corresponds to an unique point in N apart from q which is the image point of both end-points of the unit interval in N. The set N is a compact locally connected continuum with a single complementary domain and hence can be convexified. Let the corresponding distance function in N be μ. That M can be convexified follows from the [8]

THEOREM. *Let N be a compact convex metric space which is mapped continuously on the metric space M in a one-to-one fashion except for the points of the closed subset A of N all of which are sent into a single point q of M. Then M is convex with the following definition of distance:*

$$\rho(x, y) = \min. \{\mu(x', y'), \mu(x', A) + \mu(A, y')\},$$

where x is the image point in M of x' in N.

To show first that ρ is a distance function we notice that if $x = y$, then $x' = y'$ or $x', y' \in A$ so $\rho(x, y) = 0$. If $\rho(x, y) = 0$, either $x' = y'$ since μ is a distance function, or, $\mu(x', A) + \mu(A, y') = 0$, and since A is closed, this implies that $x', y' \in A$ so $x = y = q$. The symmetry condition is obviously fulfilled.

In order to prove the triangle inequality we notice that since μ is the distance function in a metric space, we have

1) $\mu(p', q') + \mu(q', r') \geqq \mu(p', r')$,

2) $\mu(p', q') + \mu(q', A) \geqq \mu(p', A)$, $\mu(A, p') + \mu(p', q') \geqq \mu(A, q')$.

By definition of the number ρ we have

3) $\mu(p', q') \geqq \rho(p, q)$, $\mu(p', A) + \mu(A, q') \geqq \rho(p, q)$.

Now the expression $\rho(p, q) + \rho(q, r)$ is equal to the left side of one of the four following inequalities which hold by virtue of 1), 2) and 3);

α) $\mu(p', q') + \mu(q', r') \geqq \mu(p', r') \geqq \rho(p, r)$,

β) $\mu(p', q') + \mu(q', A) + \mu(A, r') \geqq \mu(p', A) + \mu(A, r') \geqq \rho(p, r)$,

γ) $\mu(p', A) + \mu(A, q') + \mu(q', r') \geqq \mu(p', A) + \mu(A, r') \geqq \rho(p, r)$,

δ) $\mu(p', A) + \mu(A, q') + \mu(q', A) + \mu(A, r') \geqq \mu(p', A) + \mu(A, r') \geqq \rho(p, r)$.

Hence ρ is a metric.

---

[8] The author is indebted to A. N. Milgram for the suggestion that the author's method would yield the following theorem in place of a special case previously given.

Next it will be shown that to distinct points x, y in M there exists a between point z. First, if $q \bar{\epsilon} x + y$ and $\rho(x, y) = \mu(x', y')$, then there exists a point z' such that $\mu(x', z') + \mu(z', y') = \mu(x', y')$ since N is convex. Hence by definition of ρ, $\rho(x, z) + \rho(z, y) \leqq \mu(x', z') + \mu(z', y') = \mu(x', y') = \rho(x, y)$. Thus by the triangle inequality z is between x and y. If $q \bar{\epsilon} x + y$ and $\rho(x, y) \neq \mu(x', y')$, then $\rho(x, y) = \mu(x', A) + \mu(A, y')$. Since $\mu(x', A) = \rho(x, q)$, we have $\rho(x, y) = \rho(x, q) + \rho(q, y)$, thus q is between x and y. Next, if $q = x$ (say), the existence of a between point to q and y must be established. Since A is compact there is a point c^1 of A such that $\mu(A, y^1) = \mu(c^1, y^1)$. Since N is convex there is a point z^1 of N for which $\rho(q, y) = \mu(c^1, z^1) + \mu(z^1, y^1) = \mu(A, y^1)$. Obviously $z^1 \bar{\epsilon} y^1 + A$, hence $z \bar{\epsilon} y + q$. Now $\rho(q, z) + \rho(z, y) \leqq \mu(c^1, z^1) + \mu(z^1, y^1) = \mu(A, y^1) = \rho(q, y)$. Thus z is between q and y.

The proof in the general case is easily established by induction. Supposing that all bounded plane continuous curves with $n - 1$ complementary domains can be convexified, let M be a curve of the same type with n complementary domains. As before, we distinguish two cases according as all boundaries of such domains are mutually exclusive or not. In the first case M is topologically equivalent to a closed domain N bounded by a circle C_1 and $n - 1$ smaller circles $C_2, C_3, \cdots, C_n$ interior to C_1.[9] The circles are mutually separated and $C_2, C_3, \cdots, C_n$ are exterior to one another. Obviously N is arc lengthwise im kleinen connected hence this case is disposed of.

If $B(R_i)B(R_j) \neq 0$, then $M + \sum_1^n R_k - (R_i + R_j)$ is a continuous curve with two complementary domains. There is no loss in taking $R_i = R_1$ as the unbounded complementary domain, for if this type can be convexified, then, by performing an inversion of the plane about an interior point of R_i all cases can be made to depend upon this one. The inversion carries M into another bounded continuous curve in a one-to-one bi-continuous manner which does come under the special type being considered. If $q \epsilon B(R_1)B(R_2)$, then $M^1 = M + R_3 + R_4 + R_5 + \cdots + R_n$ is bounded and has two complementary domains. We construct next a set N on the unit interval which is carried by the transformation T into M^1, as in the case $n = 2$. Since N has one complementary domain, the set N minus the counterimages of $R_3, R_4, \cdots, R_n$, which we may call N^*, has the property of being a bounded continuous curve with $n - 1$ domains. Moreover, T carries N^* into M in a continuous fashion which is one-to-one except for the points of the closed subset A consisting of the end-points of the unit interval in N^* which are both mapped into the point q.

[9] B. V. Kerekjarto, *loc. cit.*

By assumption N^* is convex with respect to the distance function μ, hence applying the theorem given above on mappings of a convex space we conclude that M is convex with respect to the distance function $\rho(x,y)$.

4. By a regular curve is meant a bounded continuum M such that each point p of M is contained in arbitrarily small neighborhoods V such that $B(V)M$ consists of a finite set of points. If the sum of a regular curve M and an arbitrary regular curve M^1 (such that $MM^1 \neq 0$) is again a regular curve, M is said to be bestandig regular. Such a curve can be completely characterized in the following ways:

a) A continuum M is bestandig regular if and only if the set of its branch points A has an enclosure $\bar{A}$ which is totally disconnected:[10]

b) A continuum M is bestandig regular if and only if for an arbitrary non-degenerate sub-continuum L of M the set $M - L$ is not dense in M.[11]

From a) it is evident that each true cyclic element M of a bestandig regular curve M^1 is also bestandig regular. From b) the free arcs[10] are everywhere dense in M, and if t is any arc in M, the free arcs in M which are contained in t are everywhere dense in t. The number of free arcs such that any pair have in common at most end-points is countable since to each free arc t with end-points a and b may be associated an open set $t-(a+b)$ in M and certainly the number of open sets in M such that no two have a common point is countable. Let these free arcs be denoted by $u_1, u_2, u_3, \cdots$. The arc u_k can be regarded as a topological image of the interval I_k $(0 \leqq x \leqq 1/k^2, y = 1/k)$. If $N = \Sigma I_k$, then N is carried into Σu_k by this transformation T which carries I_k into u_k. To each arc t in M is associated a μ length which is defined to be the sum of the lengths of all intervals and sub-intervals of N whose images under T are contained in t. On account of the way in which the intervals I_k were defined and of the fact that every arc in M contains a free arc or a sub-arc of a free arc this μ length for a definite arc t is positive and finite. By means of the μ lengths a convexifying metric for M will be introduced.

Define $\rho(p,q) =$ g. l. b. of the set of μ numbers corresponding to the set of all arcs t joining p and q in M. To show that ρ is a metric we notice first that $\rho(p,p) = 0$. To show that $\rho(p,q) = 0$ implies that $p = q$ let $t_1, t_2, \cdots$ be any sequence of arcs in M joining this pair of points $(p \neq q)$. We shall show that there is a certain sub-arc common to infinitely many t_k, and, since the contribution of the μ length of this sub-arc is a certain $\delta > 0$, $\rho(p,q) > 0$.

---

[10] G. T. Whyburn, *Monatshefte f. Math. u. Phys.*, Bd. 38 (1931), S. 1.

[11] K. Menger, *Kurventheorie*, Leipzig, (1932), S. 264.

Let (t_k) be any sequence of arcs in M joining the distinct points p and q. M is bounded and lim. inf. $(t_k) \neq 0$ thus $D =$ lim. sup. (t_k) is a continuum. Letting A denote the branch points of M, the set $\bar{A}$ is totally disconnected. *If* $z \epsilon D - D\bar{A}$, then for $V(z)$ sufficiently small there are no branch points in V. Since z belongs to D, there is a sub-sequence (t_{k_i}) of (t_k) such that $\delta(t_{k_i}, z)$ tends to zero as k_i becomes infinite. If infinitely many t_{k_i} pass through z they are identical in V since there are no branch points in this set and hence the common sub-arc does exist. The alternate possibility is that MV consists of a countable set of components C_i containing a sequence of points $p_1, p_2, \cdots$ converging to z, $p_i \epsilon C_i$, but this is not possible since M is arcwise im kleinen connected.

That $\rho(p, q)$ satisfies the symmetry and triangle conditions is readily evident from the definition of ρ. To show the existence of a point r such that $\rho(p, r) + \rho(r, q) = \rho(p, q)$ let (t_k) be a sequence of arcs in M joining p and q for which the g. l. b. of the corresponding μ lengths is $\rho(p, q)$. To each t_k let z_k be the first point on the arc passing from p to q such that $\rho(p, z_k) \geqq \rho(p, q)/2$. There must be one on account of the continuity of the metric. If a certain z_k occurs infinitely often, set $r = z_k$, otherwise let $r \epsilon \overline{\Sigma z_k}$. Then r is between p and q. For, if $\rho(p, r) = \rho(p, q)/2 - \epsilon$, $\epsilon > 0$, we have a contradiction since $\rho(p, \text{lim. } z_{k_i}) = \text{lim. } \rho(p, z_{k_i}) \geqq \rho(p, q)/2$, as k_i increases indefinitely, where (z_{k_i}) converges to r. If $\rho(p, r) = \rho(p, q)/2 + \epsilon$, $\epsilon > 0$, again a contradiction occurs. If (z_{k_i}) converges to r, then for $V(r)$ sufficiently small, $z_{k_i} \epsilon V$, $\rho(p, z_{k_i}) \geqq \rho(pq)/2 + \epsilon/2$; if $U \Subset V$ then for z_{k_i} in U, $\rho(p, z_{k_i}) \geqq \rho(p, q)/2 + \epsilon/2$. Now any point u preceding z_{k_i} on t_{k_i} in $V - U$ is such that $\rho(p, u) \geqq \rho(p, q)/2 + \epsilon/2$, but this contradicts the definition of z_{k_i}. Hence r is between p and q. This completes the proof that bestandig regular curves are convexifiable.

5. To show that a bounded continuous curve with a set of im kleinen cycle points C such that $\bar{C}$ is totally disconnected is convexifiable it will suffice to show that each true cyclic element is bestandig regular. Since $\bar{C}$ is totally disconnected, $M\bar{C}$ is totally disconnected, where M is a true cyclic element of the given curve. Hence our proposition is implied by the

THEOREM. *If M is a cyclic curve and $\bar{C}$ is totally disconnected, where C is the set of im kleinen cycle points of M, then M is bestandig regular.*

First, we shall show that under the given conditions M is hereditarily locally connected. If it were not, there would exist a sub-continuum K of M which is a convergence continuum. Hence the order of any point p of K is

infinite. Since $\bar{C}$ is totally disconnected we can fix our attention on a point p in K which does not belong to $\bar{C}$. But by Theorem 6 of the paper *Concerning points of continuous curves defined by certain im kleinen properties*,[12] by G. T. Whyburn, a point of a cyclic curve which is not an im kleinen cycle point is a point of finite order, hence p does not belong to K. Now to show that M is bestandig regular it will be sufficient to show that there can be no sub-continuum L in $\bar{A}$, where A is the set of branch points of M. If there were such a sub-continuum, it would be a continuous curve itself since M is hereditarily locally connected, and as such it would necessarily contain an arc t. The arc t is composed of branch points and limit points of branch points of M. Since $\bar{C}$ is totally disconnected, C is not dense on t hence not uncountably dense on t, thus by Corollary 1, ¶ 3 of the paper referred to above, the arc t contains an arc segment which is an open subset of M. Hence an arc t with the above supposed properties can not exist. Thus M is bestandig regular.

OREGON STATE COLLEGE.

[12] *Mathematische Annalen*, Bd. 102, pp. 317-321.

CERTAIN MEAN VALUE THEOREMS, WITH APPLICATIONS IN THE THEORY OF HARMONIC AND SUBHARMONIC FUNCTIONS.*[1]

By F. W. Perkins.

Introduction. The purpose of this paper is to investigate the properties and uses of a certain type of integral mean. Let $f(t)$ be any real single valued function, continuous on the interval $0 \leqq t \leqq a$ of the real variable t. The expression $\phi(\alpha, \beta, \rho; f)$ studied in Part I, represents (in general) a weighted arithmetic mean of the values of $f(t)$ on the interval $0 < t < \rho$. The weighting function depends on the variables α, β and ρ. The function $\phi(\alpha, \beta, \rho; f)$ is related to the Laplace Integral, and to certain expressions used in the theory of summability.[2]

In Part II we discuss applications of the previously developed theory. Given any function u, continuous in a finite region R of the plane or of space, we define $f_P(t)$ as the arithmetic mean of u on the boundary of the circle or sphere with center at an interior point P of R and sufficiently small radius t. Through properties of $\phi(\alpha, \beta, \rho; f_P)$ we obtain a number of mean value theorems for harmonic and continuous subharmonic functions.[3] Although the most interesting applications explicitly given involve merely $\phi(1, \beta, \rho; f_P)$, some results may be obtained which involve $\phi(\alpha, \beta, \rho; f_P)$ for general values of α. We do not consider superharmonic functions, since their properties can be inferred directly from those of subharmonic functions.

---

* Received September 1, 1937; Revised June 8, 1938, September, 1938.

[1] Some of the results contained in this paper were announced by the author at the International Congress at Oslo in 1936. F. W. Perkins, "Mean value theorems with applications in the theory of harmonic, subharmonic and superharmonic functions," *Comptes Rendus du Congrès International des Mathématiciens*, Oslo, 1936, Tome II (1937), pp. 64, 65.

[2] See, for example, L. L. Silverman, "The equivalence of certain regular transformations," *Transactions of the American Mathematical Society*, vol. 26 (1924), pp. 101-112.

[3] For brief discussions (with bibliographical references) of known mean value properties of harmonic and subharmonic functions, see the following publications: G. Bouligand, "Fonctions harmoniques. Principes de Picard et de Dirichlet," *Mémorial des sciences mathématiques*, Fascicule XI, Paris (1926); see particularly pp. 4-6 inc.; T. Radó, "Subharmonic functions," *Ergebnisse der Mathematik und ihrer Grenzgebiete*, Bd. 5, Heft 1, Berlin (1937); see particularly Chapter II.

PART I: Properties of $\phi(\alpha,\beta,\rho;f)$.

1. Definition and fundamental properties of $\phi(\alpha,\beta,\rho;f)$. We give first the following definition:

Definition. *Corresponding to a given function $f(t)$, real, single valued and continuous on the interval I: $0 \leqq t \leqq a$ of the real variable t, we define a function $\phi(\alpha,\beta,\rho;f)$ for certain values of the real variables α, β and ρ by the following relations:* [4]

$$\phi(\alpha,\beta,\rho;f) = \frac{\beta^a}{\rho^\beta\Gamma(\alpha)}\int_0^\rho f(t)t^{\beta-1}\left(\log\frac{\rho}{t}\right)^{\alpha-1}dt, \tag{1}$$

when $0 < \alpha$, $0 < \beta$ and $0 < \rho \leqq a$;

$$\phi(0,\beta,\rho;f) = f(\rho), \quad \textit{when } 0 < \beta \textit{ and } 0 \leqq \rho \leqq a; \tag{2}$$

$$\phi(\alpha,0,\rho;f) = f(0), \quad \textit{when } 0 \leqq \alpha \textit{ and } 0 \leqq \rho \leqq a; \tag{3}$$

$$\phi(\alpha,\beta,0;f) = f(0), \quad \textit{when } 0 \leqq \alpha \textit{ and } 0 \leqq \beta. \tag{4}$$

Throughout this paper we are concerned only with real quantities, and in theorems relating to $\phi(\alpha,\beta,\rho;f)$ the function $f(t)$ will be assumed (without further explicit statement) to be single valued and continuous on the interval I: $0 \leqq t \leqq a$.

From (1) and (4) we have also

$$\phi(\alpha,\beta,\rho;f) = \frac{1}{\Gamma(\alpha)}\int_0^\infty f(\rho e^{-\gamma/\beta})\gamma^{a-1}e^{-\gamma}d\gamma, \tag{5}$$

when $0 < \alpha$, $0 < \beta$ and $0 \leqq \rho \leqq a$.

If $f(t) = 1$ when $0 \leqq t \leqq a$, then $\phi(\alpha,\beta,\rho;f) = 1$ when $0 \leqq \alpha$, $0 \leqq \beta$ and $0 \leqq \rho \leqq a$. Moreover the inequality

$$G_1 < f(t) < G_2$$

implies the inequality

$$G_1 < \phi(\alpha,\beta,\rho;f) < G_2, \qquad 0 \leqq \alpha,\ 0 \leqq \beta,\ 0 \leqq \rho \leqq a.$$

Let $f_0(t), f_1(t), f_2(t), \cdots, f_n(t)$ be $n+1$ functions, each continuous on I, and let $c_0, c_1, c_2, \cdots, c_n$ be $n+1$ constants. If

$$f(t) = \sum_{k=0}^{k=n} c_k f_k(t), \qquad 0 \leqq t \leqq a,$$

[4] The absolute convergence of the integral in (1) becomes obvious on making the substitution $t = \rho e^{-\gamma/\beta}$.

then

$$\phi(\alpha, \beta, \rho; f) = \sum_{k=0}^{k=n} c_k \phi(\alpha, \beta, \rho; f_k), \qquad 0 \leqq \alpha,\ 0 \leqq \beta,\ 0 \leqq \rho \leqq a.$$

In particular, if $f(t)$ is a polynomial of degree n,

$$f(t) = p_n(t) = \sum_{k=0}^{k=n} c_k t^k, \qquad 0 \leqq t \leqq a,$$

we have

$$\phi(\alpha, \beta, \rho; p_n) = \sum_{k=0}^{k=n} c_k \left(\frac{\beta}{\beta + k}\right)^{\alpha} \rho^k, \qquad 0 \leqq \alpha,\ 0 < \beta,\ 0 \leqq \rho \leqq a,$$

and

$$\phi(\alpha, 0, \rho; p_n) = c_0, \qquad 0 \leqq \alpha,\ 0 \leqq \rho \leqq a.$$

We also note that if a constant B is chosen so that

$$| f_1(t) - f_2(t) | \leqq B, \qquad 0 \leqq t \leqq a,$$

then

$$(6) \quad | \phi(\alpha, \beta, \rho; f_1) - \phi(\alpha, \beta, \rho; f_2) | \leqq B, \qquad 0 \leqq \alpha,\ 0 \leqq \beta,\ 0 \leqq \rho \leqq a.$$

By considering first the case in which $f(t)$ is a polynomial and then using Weierstrass' polynomial approximation theorem, we obtain the results given below in Theorems 1 and 2:

THEOREM 1. *The expression $\phi(\alpha, \beta, \rho; f)$ represents a continuous function of α, β and ρ throughout the region*

$$0 \leqq \alpha, \qquad 0 \leqq \beta, \qquad 0 \leqq \rho \leqq a,$$

except along the line segment

$$\alpha = 0, \qquad \beta = 0, \qquad 0 < \rho \leqq a.$$

If β and ρ are constant and α becomes positively infinite then $\phi(\alpha, \beta, \rho; f)$ approaches the limit $f(0)$:

$$\phi(+\infty, \beta, \rho; f) = \lim_{\alpha \to +\infty} \phi(\alpha, \beta, \rho; f) = f(0).$$

If α and ρ are constant and β becomes positively infinite, then $\phi(\alpha, \beta, \rho; f)$ approaches the limit $f(\rho)$:

$$\phi(\alpha, +\infty, \rho; f) = \lim_{\beta \to +\infty} \phi(\alpha, \beta, \rho; f) = f(\rho).$$

THEOREM 2. *Let α', $\bar{\alpha}$ and β' be any non-negative constants, and let*

$$f'(t) = \phi(\alpha', \beta', t; f), \quad \textit{when} \quad 0 \leqq t \leqq a.$$

Then

$$\phi(\bar{\alpha}, \beta', \rho; f') = \phi(\alpha' + \bar{\alpha}, \beta', \rho; f), \quad \textit{when} \quad 0 \leqq \rho \leqq a.$$

THEOREM 3. *For values* α, β *and* ρ *such that*

$$0 \leqq \alpha, \quad 0 < \beta \quad and \quad 0 \leqq \rho \leqq a,$$

the function $\phi(\alpha, \beta, \rho; f)$ *has a continuous first partial derivative with respect to* β, *and*

$$\frac{\partial}{\partial \beta}\phi(\alpha, \beta, \rho; f) = \frac{\alpha}{\beta}[\phi(\alpha, \beta, \rho; f) - \phi(\alpha + 1, \beta, \rho; f)]. \tag{7}$$

For values of α, β *and* ρ *such that*

$$1 \leqq \alpha, \quad 0 \leqq \beta \quad and \quad 0 < \rho \leqq a,$$

the function $\phi(\alpha, \beta, \rho; f)$ *has a continuous first partial derivative with respect to* ρ, *and*

$$\frac{\partial}{\partial \rho}\phi(\alpha, \beta, \rho; f) = \frac{\beta}{\rho}[\phi(\alpha - 1, \beta, \rho; f) - \phi(\alpha, \beta, \rho; f)]. \tag{8}$$

It is readily verified that this theorem is true when $f(t)$ is a polynomial, and it is possible to determine an infinite sequence of polynomials $p^{(1)}(t)$, $p^{(2)}(t)$, $p^{(3)}(t), \cdots$, which converges uniformly on I to $f(t)$. Using (6) we see that when $0 \leqq \alpha$, $0 < \beta$ and $0 \leqq t \leqq a$,

$$\lim_{i \to \infty} \phi(\alpha, \beta, \rho; p^{(i)}) = \phi(\alpha, \beta, \rho; f),$$

and so

$$\lim_{i \to \infty} \frac{\partial}{\partial \beta}\phi(\alpha, \beta, \rho; p^{(i)}) = \frac{\alpha}{\beta}[\phi(\alpha, \beta, \rho; f) - \phi(\alpha + 1, \beta, \rho; f)];$$

moreover, for fixed α and ρ the convergence is in each case uniform with respect to β on any interval $\beta' \leqq \beta \leqq \beta''$, where β' and β'' are positive constants. Hence $\partial\phi(\alpha, \beta, \rho; f)/\partial\beta$ exists and is given by (7). The relation (8) may be established by a similar method. Finally, the continuity of these partial derivatives follows from known properties of boundedness and continuity of $\phi(\alpha, \beta, \rho; f)$.

2. Further properties of $\phi(\alpha, \beta, \rho; f)$. This section is devoted to properties of $\phi(\alpha, \beta, \rho; f)$ which will prove useful in the discussion of applications.

THEOREM 4. *If* α', β' *and* ρ' *are constants such that*

$$0 \leqq \alpha', \quad 0 \leqq \beta' \quad and \quad 0 \leqq \rho' \leqq a,$$

and if $f(t)$ *is a non-decreasing function of* t *on the interval* $0 \leqq t \leqq a$, *then*

(i), $\phi(\alpha, \beta', \rho'; f)$ *is a non-increasing function of* α *on the interval* $0 \leqq \alpha$,

(ii), *$\phi(\alpha', \beta, \rho'; f)$ is a non-decreasing function of β on the interval* $0 \leqq \beta$.

(iii), *$\phi(\alpha', \beta', \rho; f)$ is a non-decreasing function of ρ on the interval* $0 \leqq \rho \leqq a$.

The theorem is obviously true if at least one of the constants α', β' and ρ' is zero, and so we may exclude this case from further consideration.

To establish (i) for the case in which $0 < \beta'$ and $0 < \rho' \leqq a$, we first let α_1 and α_2 be any two constants such that $0 < \alpha_1 < \alpha_2$ and note that there then exists a positive constant γ_0 uniquely determined by the condition

$$\Gamma(\alpha_2) - \gamma_0^{\alpha_2 - \alpha_1}\Gamma(\alpha_1) = 0.$$

Referring to (5) we may write

$$\begin{aligned}\Gamma(\alpha_1)\Gamma(\alpha_2)&[\phi(\alpha_1, \beta', \rho'; f) - \phi(\alpha_2, \beta', \rho'; f)] \\ &= \{\int_0^{\gamma_0} + \int_{\gamma_0}^{\infty}\} f(\rho' e^{-\gamma/\beta'})[\Gamma(\alpha_2) - \gamma^{\alpha_2-\alpha_1}\Gamma(\alpha_1)]\gamma^{\alpha_1-1}e^{-\gamma}d\gamma \\ &\geqq f(\rho' e^{-\gamma_0/\beta'})\int_0^{\infty} e^{-\gamma}\gamma^{\alpha_1-1}[\Gamma(\alpha_2) - \gamma^{\alpha_2-\alpha_1}\Gamma(\alpha_1)]d\gamma.\end{aligned}$$

But the integral in the last line of the above formula has the value zero, and so

$$\phi(\alpha_2, \beta', \rho'; f) \leqq \phi(\alpha_1, \beta', \rho'; f).$$

By holding α_2 fast and allowing α_1 to approach zero as a limit we see that this relation is also valid if $\alpha_1 = 0$. This completes the proof of (i).

The validity of (ii) is readily established through (i) and (7).

To prove that (iii) is valid when $0 < \alpha'$ and $0 < \beta'$ we note that if $0 \leqq \rho_1 \leqq \rho_2 \leqq a$, then

$$\begin{aligned}&\phi(\alpha', \beta', \rho_2; f) - \phi(\alpha', \beta', \rho_1; f) \\ &= \frac{1}{\Gamma(\alpha')}\int_0^{\infty}[f(\rho_2 e^{-\gamma/\beta'}) - f(\rho_1 e^{-\gamma/\beta'})]\gamma^{\alpha'-1}e^{-\gamma}d\gamma \geqq 0,\end{aligned}$$

which yields the desired result.

THEOREM 5. *If there exist a positive constant α' and a non-negative constant β' such that $\phi(\alpha', \beta', \rho; f) \leqq f(\rho)$, when $0 \leqq \rho \leqq a$, then $f(t)$ attains its minimum value on $I: 0 \leqq t \leqq a$ at $t = 0$.*

If the theorem is false, there exists a constant ρ' such that $0 < \rho' \leqq a$ and $f(\rho') < f(t)$ when $0 \leqq t < \rho'$. Since $\phi(\alpha', \beta', \rho'; f)$ is either $f(0)$ or a weighted mean of the values of $f(t)$ on the interval $0 < t < \rho'$ this implies that

$$f(\rho') < \phi(\alpha', \beta', \rho'; f),$$

which is inconsistent with the hypothesis of the theorem.

THEOREM 6. *If there exist constants β' and β'' such that*

(9) $\quad 0 \leqq \beta' < \beta''$ *and* $\phi(1,\beta',\rho;f) \leqq \phi(1,\beta'',\rho;f)$, *when* $0 \leqq \rho \leqq a$,

then to an arbitrary positive ϵ *there corresponds a* δ *such that*

$$0 < \delta < \epsilon, \quad \delta < a \quad \text{and} \quad f(0) \leqq f(\delta). \tag{10}$$

Furthermore, in this theorem we may replace $\phi(1,\beta'',\rho;f)$ *by its limiting value as* β'' *becomes positively infinite, that is by* $f(\rho)$.

The limiting form of this theorem, in which $\phi(1,\beta'',\rho;f)$ is replaced by $f(\rho)$, is obviously true, inasmuch as Theorem 5 tells us that in this case $f(t)$ assumes its minimum value on I at $t=0$.

In the case in which $0=\beta'<\beta''$, the relations (9), (1) and (3) yield

$$0 \leqq \frac{\beta''}{\rho^{\beta''}}\int_0^\rho [f(t)-f(0)]t^{\beta''-1}dt, \qquad 0<\rho\leqq a.$$

Setting ρ equal to the smaller of ϵ and a (or their common value if $\epsilon = a$) we see from the first law of the mean that there exists a δ satisfying the requirements (10).

As the first step in the consideration of the case in which $0<\beta'<\beta''$, we establish the following lemma:

LEMMA. *If* β' *and* β'' *are positive constants and if* $0<\rho\leqq a$, *then*

$$\phi(1,\beta'',\rho;f) = \frac{\beta''}{\beta'}\left[\phi(1,\beta',\rho;f) - \frac{\beta''-\beta'}{\rho^{\beta''}}\int_0^\rho t^{\beta''-1}\phi(1,\beta',t;f)dt\right]. \tag{11}$$

Using (8) and (2) we see that

$$\beta'\beta''[\phi(1,\beta'',\rho;f)-\phi(1,\beta',\rho;f)] + \rho\beta'\frac{\partial}{\partial\rho}[\phi(1,\beta'',\rho;f)-\phi(1,\beta',\rho;f)]$$
$$= (\beta''-\beta')\rho\frac{\partial}{\partial\rho}\phi(1,\beta',\rho;f).$$

After multiplying by $\rho^{\beta''-1}$ and integrating we have

$$\beta'\rho^{\beta''}[\phi(1,\beta'',\rho;f)-\phi(1,\beta',\rho;f)] = (\beta''-\beta')\int_0^\rho t^{\beta''}\frac{\partial}{\partial t}\phi(1,\beta',t;f)dt.$$

Through integration by parts we see that

$$\int_0^\rho t^{\beta''}\frac{\partial}{\partial t}\phi(1,\beta',t;f)dt = \rho^{\beta''}\phi(1,\beta',\rho;f) - \beta''\int_0^\rho t^{\beta''-1}\phi(1,\beta',t;f)dt.$$

From the last two equations we obtain the desired relation, (11).

Returning to the consideration of the theorem for the case in which $0<\beta'<\beta''$, we see that in this case (9) and the lemma yield

$$0 \leqq \frac{\beta'' - \beta'}{\beta'} [\phi(1, \beta', \rho; f) - \frac{\beta''}{\rho^{\beta''}} \int_0^\rho t^{\beta''-1} \phi(1, \beta', t; f) dt], \quad 0 < \rho \leqq a,$$

or, multiplying by the positive quantity $\beta' \rho^{\beta''} / \beta''(\beta'' - \beta')$,

$$(12) \qquad 0 \leqq \int_0^\rho t^{\beta''-1} [\phi(1, \beta', \rho; f) - \phi(1, \beta', t; f)] dt, \quad 0 < \rho \leqq a.$$

From this it follows that $\phi(1, \beta', t; f)$ attains its minimum value on I at $t = 0$, for otherwise there would exist a constant ρ' such that $0 < \rho' \leqq a$ and

$$\phi(1, \beta', \rho'; f) < \phi(1, \beta', t; f), \qquad 0 \leqq t < \rho',$$

and on setting $\rho = \rho'$ in (12) we should have a contradiction. Hence

$$\phi(1, \beta', 0; f) \leqq \phi(1, \beta', t; f), \qquad 0 \leqq t \leqq a,$$

which may also be written in the form

$$\phi(1, 0, t; f) \leqq \phi(1, \beta', t; f), \qquad 0 \leqq t \leqq a.$$

Except for difference in notation, this is the hypothesis of the previously considered case in which $\beta' = 0$, and so implies the validity of the theorem for the case in which $0 < \beta' < \beta''$.

THEOREM 7. *If there exist constants α', α'' and β' such that*

$$0 \leqq \alpha' < \alpha'', \qquad 0 < \beta'$$

and

$$(13) \qquad \phi(\alpha'', \beta', \rho; f) \leqq \phi(\alpha', \beta', \rho; f), \text{ when } 0 \leqq \rho \leqq a,$$

then to an arbitrary positive ϵ, there corresponds a δ such that

$$0 < \delta < \epsilon, \quad \delta < a \quad \text{and} \quad f(0) \leqq f(\delta).$$

Furthermore, in this theorem we may replace $\phi(\alpha'', \beta', \rho; f)$ by its limiting value as α'' becomes positively infinite, that is by $f(0)$.

In the limiting form of the theorem we assume that

$$f(0) \leqq \phi(\alpha', \beta', \rho; f), \qquad 0 \leqq \rho \leqq a.$$

If $\alpha' = 0$ the desired result is immediately obtained; if $0 < \alpha'$ then $\phi(\alpha', \beta', \rho; f)$ is a weighted mean of the values of the continuous function $f(t)$ on the interval $0 < t < \rho$. Hence, denoting by ϵ' the smaller of the constants ϵ and a (or their common value if $\epsilon = a$) there exists a constant δ such that

$$0 < \delta < \epsilon', \qquad f(\delta) = \phi(\alpha', \beta', \epsilon'; f).$$

and so,

$$f(0) \leqq f(\delta).$$

Hence the theorem is valid in the limiting form.

Turning now to the case in which (13) is assumed, we set $\bar{\alpha} = \alpha'' - \alpha'$ and

$$f'(t) = \phi(\alpha', \beta', t; f), \qquad 0 \leqq t \leqq a.$$

Using Theorem 2, we see that (13) may be written in the form

$$\phi(\bar{\alpha}, \beta', \rho; f') \leqq f'(\rho), \qquad 0 \leqq \rho \leqq a.$$

Using Theorem 5 we have

$$f'(0) \leqq f'(\rho), \qquad 0 \leqq \rho \leqq a,$$

that is,

$$f(0) \leqq \phi(\alpha', \beta', \rho; f), \qquad 0 \leqq \rho \leqq a.$$

We have already shown that this inequality implies the desired result, and so the proof is complete.

THEOREM 8. *Let α' be a non-negative constant and β' a positive constant, and set*

$$f'(t) = \phi(\alpha', \beta', t; f), \text{ when } 0 \leqq t \leqq a.$$

If it is possible to choose α' and β' (subject to the above restrictions) so that

$$\phi(1, 1, \rho; f') \leqq f'(\rho), \text{ when } 0 \leqq \rho \leqq a,$$

or so that $\phi(1, 1, \rho; f')$ is a non-decreasing function of ρ on the interval $0 \leqq \rho \leqq a$, then to an arbitrary positive ϵ there corresponds a δ such that

$$0 < \delta < \epsilon, \quad \delta < a \quad \text{and} \quad f(0) \leqq f(\delta).$$

If $\phi(1, 1, \rho; f') \leqq f'(\rho)$ when $0 \leqq \rho \leqq a$, then from Theorem 5 we know that $f'(\rho)$ attains its minimum on the interval $0 \leqq \rho \leqq a$ when $\rho = 0$. Hence

$$f(0) \leqq \phi(\alpha', \beta', \rho; f), \qquad 0 \leqq \rho \leqq a,$$

and the desired result follows from the limiting form of Theorem 7.

If $\phi(1, 1, \rho; f')$ is a non-decreasing function of ρ, then

$$0 \leqq \frac{\partial}{\partial \rho} \phi(1, 1, \rho; f') = \frac{1}{\rho} [f'(\rho) - \phi(1, 1, \rho; f')],$$

when $0 < \rho \leqq a$. Noting that $f'(\rho)$ and $\phi(1, 1, \rho; f')$ are continuous when $\rho = 0$, we infer that

$$\phi(1, 1, \rho; f') \leqq f'(\rho), \qquad 0 \leqq \rho \leqq a,$$

and the desired result follows from the first part of this theorem.

PART II: Applications.

In Part II we discuss the use of the foregoing results in the study of certain properties of functions continuous in a finite region of the plane or of space.

1. Definitions. We formulate our definitions first for the spatial case, and later comment on the situation in the plane.

By a finite region R of space we mean a finite domain (that is, a bounded, open, connected set of points) of euclidean space of three dimensions, or such a domain together with some or all of its boundary points.

The finite region comprising the interior and boundary of the sphere of positive radius t with center at the interior point P of R will be denoted by $S_P(t)$.

Let u be any function which is continuous at each point of R. We define as the peripheral mean of u associated with a region $S_P(t)$ contained in R, the arithmetic mean (with respect to area) of the value of u on the boundary of $S_P(t)$. We denote this mean by $f_P(t)$ and extend the definition of $f_P(t)$ by writing $f_P(0) = u(P)$. For any fixed interior point P of R the function $f_P(t)$ is continuous for each value of t for which it is defined.

We define as the radial mean of u associated with an $S_P(\rho)$, contained in R, the value obtained by first forming the arithmetic mean of u (with respect to length) on a radial line drawn to an arbitrary element of area on the boundary of $S_P(\rho)$ and then determining the arithmetic mean of this result (with respect to area) on the surface of the sphere.

In order to define the conical mean of u associated with an $S_P(\rho)$ contained in R, we first select a directed diameter L of $S_P(\rho)$ and consider the arithmetic mean (with respect to area) of the value of u on the lateral surface of the right circular cone formed by those radial line segments of $S_P(\rho)$ which determine with L an angle θ, either acute or obtuse. The result thus obtained is now interpreted as a function of the solid angle $\Omega = 2\pi(1 - \cos\theta)$ formed by the cone at P. The arithmetic mean with respect to Ω of this result is defined as the conical mean of u associated with $S_P(\rho)$. We will show later that this mean is independent of the choice of L.

The volumetric mean of u associated with an $S_P(\rho)$ contained in R is defined as the arithmetic mean of u with respect to volume over the region $S_P(\rho)$.

In the plane it is possible, in most cases, to define concepts corresponding to those we have given in detail for the spatial case. The peripheral mean of u associated with a circular region $S_P(t)$ contained in R is computed by

forming the arithmetic mean of t with respect to arc length on the boundary of $S_P(t)$. We may set $f_P(0) = u(P)$, as before. The radial mean also has a direct analogue; the volumetric mean in space corresponds to an areal mean in the plane. The conical mean has no direct analogue in the two dimensional case.

2. Geometric interpretations. In this section we give interpretations of $\phi(1, \beta, \rho; f_P)$ for certain values of β.

THEOREM 9. *If u is a function continuous in the finite region R of space, and if a_P is a function (not necessarily continuous) of the interior point P of R such that $0 < a_P$ and $S_P(a_P) < R$, then the following interpretations are valid when $0 < \rho \leqq a_P$:*

$\phi(1, 0, \rho; f_P)$ *is the value of u at P;*
$\phi(1, 1, \rho; f_P)$ *is the radial mean of u;*
$\phi(1, 2, \rho; f_P)$ *is the conical mean of u;*
$\phi(1, 3, \rho; f_P)$ *is the volumetric mean of u;*
$\phi(1, +\infty, \rho; f_P)$ *is the peripheral mean of u.*

If R is a finite region of the plane, then

$\phi(1, 0, \rho; f_P)$ *is the value of u at P;*
$\phi(1, 1, \rho; f_P)$ *is the radial mean of u;*
$\phi(1, 2, \rho; f_P)$ *is the areal mean of u;*
$\phi(1, +\infty, \rho; f_P)$ *is the peripheral mean of u.*

Each of the means involved (in space or in the plane) is that associated with $S_P(\rho)$.

We study first the situation in space. The interpretation given for $\phi(1, 0, \rho; f_P)$ is evidently correct. In discussing some of the remaining cases, we shall find it convenient to introduce a spherical coördinate system, choosing as pole an arbitrarily selected interior point P of R, as polar axis $(\theta = 0)$ any ray drawn from P, and as the plane of the prime meridian $(\psi = 0)$ any plane through the polar axis. Let Q be any point of R with spherical coördinates (r, θ, ψ); we introduce as an alternative notation for $u(Q)$ the symbol $u(r, \theta, \psi)$. We observe now that

$$f_P(t) = \frac{1}{4\pi}\int_0^{2\pi} d\psi \int_0^{\pi} u(t, \theta, \psi) \sin\theta \, d\theta, \qquad 0 \leqq t \leqq a_P.$$

The radial mean of u associated with $S_P(\rho)$ is

$$\frac{1}{4\pi\rho}\int_0^{2\pi} d\psi \int_0^{\pi} \sin\theta\, d\theta \int_0^{\rho} u(t, \theta, \psi)\, dt.$$

By a change in the order of integration this is found to be $\phi(1, 1, \rho; f_P)$.

If L is chosen as the polar axis, the arithmetic mean of u with respect to area on the cone described in the definition of the conical mean is

$$\frac{1}{\pi\rho^2}\int_0^{\rho} t\, dt \int_0^{2\pi} u(t, \theta, \psi)\, d\psi.$$

Now $d\Omega = 2\pi \sin\theta\, d\theta$, and so for specialized L the desired conical mean is

$$\frac{2}{\rho^2}\int_0^{\rho} \frac{t dt}{4\pi}\int_0^{2\pi} d\psi \int_0^{\pi} u(t, \theta, \psi) \sin\theta\, d\theta,$$

which is $\phi(1, 2, \rho; f_P)$. The value of this expression is clearly independent of the choice of the polar axis of the coördinate system, and so represents the conical mean of u associated with $S_P(\rho)$ for any choice of L.

The properties of volumetric means are well known. It is a simple matter to verify that the volumetric mean of u associated with $S_P(\rho)$ is $\phi(1, 3, \rho; f_P)$.

The validity of the interpretation given for $\phi(1, +\infty, \rho; f_P)$ is obvious from Theorem 1.

The interpretations given for the case in which R is a finite region of the plane can be justified by methods analogous to those used in the spatial case. It should be noted that although the areal mean in the plane is the geometric analogue of the volumetric mean in space, it corresponds to a different value of β in $\phi(1, \beta, \rho; f_P)$.

We also observe that $\phi(1, 1, \rho; f_P)$ and $\phi(2, 1, \rho; f_P)$ may be interpreted as the arithmetic averages on the interval $0 < t < \rho$ of the peripheral and radial means, respectively, associated with $S_P(t)$.

3. Harmonic and subharmonic functions. We use the term "harmonic" in the classical sense,[5] and for subharmonic functions adopt the following definition, which is essentially that given by Kellogg.[6]

Let u be a function continuous in the finite region R (of the plane, or of space). Let $\mathfrak{R}$ be any closed subregion of R. Let v_1 be a function which is harmonic in $\mathfrak{R}$ and such that $u \leqq v_1$ on the boundary of $\mathfrak{R}$. If, for every

[5] See, for instance, O. D. Kellogg, *Foundations of Potential Theory*, Berlin (1929), p. 211.

[6] O. D. Kellogg, *loc. cit.*, p. 315.

such $\mathfrak{R}$ and v_1, we have $u \leqq v_1$ in the interior of $\mathfrak{R}$, we say that u is subharmonic in the interior of R.

Two known properties of subharmonic functions play an important rôle in the theory outlined in this section. Each of these properties was originally given with reference to a more general type of subharmonic function. In the form in which we shall use them, these results are contained in the two theorems stated below:

RIESZ'S THEOREM.[7] *If the function u is subharmonic in the interior of a finite region R of the plane or of space, then for each interior point P of R the function $f_P(t)$ is non-decreasing throughout the interval on which it is defined.*

LITTLEWOOD'S THEOREM.[8] *A necessary and sufficient condition that a function u, continuous in a finite region R of the plane or of space, be subharmonic in the interior of R is that, given any positive constant ϵ, to each interior point P of R there corresponds a constant δ_P such that*

$$0 < \delta_P < \epsilon, \quad S_P(\delta_P) < R \quad \textit{and} \quad u(P) \leqq f_P(\delta_P).$$

By choosing the $f(t)$ of Part I as $f_P(t)$ we obtain, with the aid of these two theorems, various results concerning subharmonic functions. Many of these results lead at once to theorems concerning harmonic functions, by virtue of the fact that a necessary and sufficient condition that u be harmonic is that both u and $-u$ be subharmonic. We give the following as an illustrative example:

THEOREM 10. *Let u be a given function, continuous in a finite region R of the plane or of space. If u is subharmonic in the interior of R and if to each interior point P of R we assign constants a_P, β'_P and β''_P such that*

$$0 < a_P, \quad S_P(a_P) < R \quad \textit{and} \quad 0 \leqq \beta'_P < \beta''_P,$$

then

$$\phi(1, \beta'_P, \rho; f_P) \leqq \phi(1, \beta''_P, \rho; f_P), \quad \textit{when} \quad 0 \leqq \rho \leqq a_P.$$

Conversely, if to each interior point P of R there correspond constants a_P, β'_P and β''_P satisfying the conditions given above and, further, such that

$$\phi(1, \beta'_P, \rho; f_P) \leqq \phi(1, \beta''_P, \rho, f_P), \quad \textit{when} \quad 0 \leqq \rho \leqq a_P,$$

[7] F. Riesz, "Sur les fonctions subharmoniques et leur rapport à la théorie du potentiel," II, *Acta Mathematica*, vol. 54 (1930), pp. 321-360. See also T. Radó, *loc. cit.*, paragraph 2. 4.

[8] J. E. Littlewood, "On the definition of subharmonic functions," *Journal of the London Mathematical Society*, vol. 2 (1927), p. 189 ff. See also T. Radó, *loc. cit.*, paragraphs 1. 6 and 2. 1–2. 3 inc.

then u is subharmonic in the interior of R. Furthermore, throughout this theorem we may replace $\phi(1, \beta''_P, \rho; f_P)$ by $f_P(\rho)$ for some or all points P.

In this theorem we may substitute the word "harmonic" for "subharmonic," provided that we write

$$\phi(1, \beta'_P, \rho; f_P) = \phi(1, \beta'', \rho; f_P), \quad \textit{when} \quad 0 \leqq \rho \leqq a_P,$$

and

$$\phi(1, \beta'_P, \rho; f_P) = f_P(\rho), \quad \textit{when} \quad 0 \leqq \rho \leqq a_P,$$

in place of the corresponding inequalities.[9]

Interesting results may be obtained as particular cases of this theorem, in either two or three dimensions. For example, if u is subharmonic in the interior of a finite region R of space, then the means of u associated with any $S_P(\rho)$ contained in R satisfy the following inequalities:

$$u(P) \leqq \textit{radial mean} \leqq \textit{conical mean}$$
$$\leqq \textit{volumetric mean} \leqq \textit{peripheral mean},$$

and conversely, if for each interior point P of R some pair of these quantities satisfy (for all sufficiently small positive ρ) a weak inequality corresponding to their position in the scheme given above, then u is subharmonic.[10]

Our final theorem gives a condition that u be subharmonic which contains as special cases several results due to Littlewood.[11]

THEOREM 11. *Let u be a function continuous in a finite region R of the plane or of space. A necessary and sufficient condition that u be subharmonic in the interior of R is that to each interior point P of R there correspond a positive constant a_P such that $S_P(a_P) < R$, and three sequences of constants*

$$\alpha_P{}^{(1)}, \alpha_P{}^{(2)}, \alpha_P{}^{(3)}, \cdots; \quad \beta_P{}^{(1)}, \beta_P{}^{(2)}, \beta_P{}^{(3)}, \cdots; \quad \textit{and} \quad \rho_P{}^{(1)}, \rho_P{}^{(2)}, \rho_P{}^{(3)}, \cdots;$$

---

[9] Compare the implications of the condition $u(P) = \phi(1, 0, \rho; f_P) = \phi(1, \beta''_P, \rho; f_P)$ with the theorems on mediation quoted by Bouligand, *loc. cit.*, pp. 4-6.

[10] Necessary and sufficient conditions that u be subharmonic given in previously published papers include the inequalities

$$u(P) \leqq \textit{peripheral} \text{ or } \textit{areal} \text{ (or } \textit{volumetric}\text{) } \textit{mean},$$

due to J. E. Littlewood, (*loc. cit.*) and the inequality

$$\textit{areal} \text{ (or } \textit{volumetric}\text{) } \textit{mean} \leqq \textit{peripheral mean},$$

given by E. F. Bechenbach, and T. Radó, "Subharmonic functions and surfaces of negative curvature," *Transactions of the American Mathematical Society*, vol. 35 (1933), pp. 662-674. See also T. Radó, "Subharmonic functions," paragraphs 2.8 (p. 8) and 3.25 (p. 19).

[11] J. E. Littlewood, *loc. cit.*

such that

$$0 \leqq \alpha_P^{(k)},\ 0 < \beta_P^{(k)},\ 0 < \rho_P^{(k)} \leqq a_P,\ (k = 1, 2, 3, \cdots), \qquad \lim_{k\to\infty} \rho_P^{(k)} = 0,$$

and

$$(14) \qquad u(P) \leqq \phi(\alpha_P^{(k)}, \beta_P^{(k)}, \rho_P^{(k)}; f_P), \qquad (k = 1, 2, 3, \cdots).$$

The necessity of the condition is obvious from Theorem 4. To demonstrate the sufficiency we note that given any positive integer k there exists a $\delta_P^{(k)}$ such that

$$0 < \delta_P^{(k)} \leqq \rho_P^{(k)} \quad \text{and} \quad \phi(\alpha_P^{(k)}, \beta_P^{(k)}, \rho_P^{(k)}; f_P) = f_P(\delta_P^{(k)}),$$

and so, given any $\epsilon > 0$ there exists a δ_P such that

$$0 < \delta_P < \epsilon, \quad S_P(\delta_P) < R \quad \text{and} \quad u(P) \leqq f_P(\delta_P),$$

whence we obtain the desired result through Littlewood's Theorem.

We note that to obtain a corresponding necessary and sufficient condition that u be harmonic we need only replace the inequalities (14) by equations.

COROLLARY. *A necessary and sufficient condition that a function u, continuous in a finite region R of the plane or of space, be subharmonic in the interior of R is that to each interior point P of R there correspond constants a_P, α'_P and β'_P satisfying the conditions*

$$0 < a_P, \quad S_P(a_P) < R, \quad 0 \leqq \alpha'_P \quad \text{and} \quad 0 < \beta'_P,$$

and such that $\phi(\alpha'_P, \beta'_P, \rho; f_P)$ is a non-decreasing function of ρ on the interval $0 \leqq \rho \leqq a_P$.

We note that if we replace the words "non-decreasing function of ρ" by "independent of ρ" we obtain a necessary and sufficient condition that u be harmonic in the interior of R.

DARTMOUTH COLLEGE,
HANOVER, N. H.

ON THE SMOOTHNESS OF INFINITE CONVOLUTIONS OF THE TYPE OCCURRING IN THE THEORY OF THE RIEMANN ZETA-FUNCTION.*

By Aurel Wintner.

The smoothness of infinite convolutions of the type mentioned in the title has been treated by an estimate of Fourier-Stieltjes transforms of the distributions on convex curves (cf. Wintner [4], pp. 328-329; Jessen and Wintner [2]). The method of obtaining such an estimate consisted in an extension of the usual estimate of the Bessel functions J_n, and has used, besides a lemma of van der Corput, the assumption that the spectra are sufficiently smooth convex curves. The resulting estimate has then been refined in such a way as to yield an asymptotic formula also (Haviland and Wintner [1]). The methods applied are decidedly restricted to the convex analytic case and to a two-dimensional distribution. Also they represent quite a complicated part of the theory, developed *loc. cit.* [2]. In fact, this part and only this part of the theory had to be restricted to the two-dimensional case (*loc. cit.* [2]).

The object of the present paper is to develop a simpler and more general method, which is free of the restrictions of the dimensionality, analyticity, and convexity, and is quite elementary in nature. The method is adapted to the cases of the type occurring in connection with Dirichlet series in the theory of numbers. Actually, it does not yield any information in case of finite convolutions. Correspondingly, the method applies precisely in those cases in which it supplies corresponding smoothness properties for Bernoulli convolutions also (cf. Wintner [5]).

Let Σ be a set in a j-dimensional real vector space, and let e denote an arbitrary point of Σ. In order to simplify the manner of speaking, it will be assumed that Σ is the sphere $|e| = 1$, formed by all unit vectors e. Lebesgue integrals over whole Σ will be denoted by $\int \cdots d\Sigma_e$. The areal measure on Σ will be thought of as normalized by introduction of a constant factor in such a way that the area $\int d\Sigma_e$ of Σ becomes unity.

Let f be a (real) vector function with k ($\gtreqless j$) components, which is defined as a function of the position ρe in the interior of Σ; so that $0 \leqq \rho < 1$. Suppose that $f = f(\rho e)$ is, for every fixed ρ, a measurable function on Σ. For every ρ, the mapping $x = f(\rho e)$ of Σ determines in a k-dimensional euclidean

* Received October 7, 1938.

x-space an absolutely additive set-function $\phi_\rho = \phi_\rho(E)$, defined for every Borel set E of the x-space as the Σ-measure of the set of those points e at which $x = f(\rho e)$ belongs to E. Since

$$\int d\Sigma_e = 1, \tag{1}$$

$\phi_\rho(E)$ is a distribution function. Denoting by u an arbitrary point of another real k-dimensional euclidean space, and by $\Lambda(u) = \Lambda(u; \psi)$ the Fourier-Stieltjes transform of a distribution function $\psi = \psi(E)$ on the x-space, one readily sees that

$$\Lambda(u; \phi_\rho) = \int \exp\{iu \cdot f(\rho e)\} d\Sigma_e, \tag{2}$$

where the period denotes scalar multiplication.

It will be assumed that $\phi_\rho(E)$ has a finite standard deviation, that is, that the expectation value of $x^2 = x \cdot x$ is not $+\infty$. In view of (2), this will be the case if and only if the function $f(\rho e)$ of the position e on Σ is of class L^2 for every fixed ρ. As far as the k moments of the first order are concerned, the center of the mass distribution $\phi_\rho(E)$ will be assumed to be the origin of the x-space for every ρ; so that the expectation of x is the 0-vector. According to (2), the condition which is imposed on $f(\rho e)$ by this normalization is that

$$\int f(\rho e) d\Sigma_e = 0 \tag{3}$$

for every ρ.

It will also be assumed that $f(\rho e)$ is in the neighborhood of the center of Σ of the form

$$f(\rho e) = \rho g(e) + o(\rho), \tag{4}$$

where $g = g(e)$ is some (vector) function which is independent of the distance ρ, and the o-term is meant to hold uniformly for all directions e. Since the function g of the position e on Σ clearly is of class L^2,

$$\kappa(u) = \int [u \cdot g(e)]^2 d\Sigma_e \tag{4 bis}$$

defines a quadratic form in the k components of u.

Finally, it will be assumed that the non-negative definite quadratic form (4 bis) is positive definite.

Since $| u \cdot f |^2 \leqq u^2 f^2$,

$$\exp\{i u \cdot f\} = 1 + i u \cdot f - \tfrac{1}{2}(u \cdot f)^2 + o(u^2 f^2) \text{ as } u^2 f^2 \to 0.$$

Hence, from (2), (1) and (3),

$$\Lambda(u; \phi_\rho) = 1 - \tfrac{1}{2}\int [u \cdot f(\rho e)]^2 d\Sigma_e + \int o(u^2 f(\rho e)^2) d\Sigma_e.$$

Since (4) holds uniformly in e, it follows that

$$\Lambda(u;\phi_\rho) = 1 - \tfrac{1}{2}\int[\rho u\cdot g(e) + o(\rho\,|\,u\,|)]^2 d\Sigma_e + o(\rho^2 u^2) \quad \text{as } \rho\,|\,u\,| \to 0.$$

But $g(e)$ is of class L^2 on Σ; so that, on using the notation (4 bis) and the inequality of Schwarz,

$$\Lambda(u;\phi_\rho) = 1 - \tfrac{1}{2}\rho^2\kappa(u) + o(\rho^2 u^2) \quad \text{as } \rho\,|\,u\,| \to 0.$$

This means that $\log\Lambda(u;\phi_\rho) = -\tfrac{1}{2}\rho^2\kappa(u) + o(\rho^2u^2)$; so that

(5) $$\Lambda(u;\phi_\rho) = \exp\{-\tfrac{1}{2}\rho^2\kappa(u) + o(\rho^2u^2)\}, \text{ as } \rho\,|\,u\,| \to 0.$$

Now choose a fixed sequence $\rho_1, \rho_2, \cdots$ of positive numbers ρ_n which tend with $1/n$ to zero, and denote the distribution function $\phi_\rho = \phi_\rho(E)$ belonging to $\rho = \rho_n$ simply by $\phi_n = \phi_n(E)$. Denoting by α the minimum, by β the maximum of the positive definite quadratic form (4 bis) on the sphere $|\,u\,| = 1$, one has

(6) $$\alpha u^2 \leqq \kappa(u) \leqq \beta u^2 \qquad (0 < \alpha \leqq \beta;\ u^2 = u\cdot u = |\,u\,|^2)$$

for every u. Hence it is clear from (5) and from the assumption

(7) $$\rho_n \to 0, \qquad (n \to \infty),$$

that the infinite product $\prod_{n=1}^{\infty}\Lambda(u;\phi_n)$ is uniformly convergent in every or in no sphere $|\,u\,| <$ const. of the u-space according as the series

(8) $$\sum_{n=1}^{\infty}\rho_n^2$$

is convergent or divergent. This means that the infinite convolution

(9) $$\phi(E) = \phi_1(E) * \phi_2(E) * \cdots * \phi_n(E) * \cdots$$

is convergent if and only if so is the numerical series (8). [This fact is not implied by the general theory of infinite convolutions (cf. Jessen and Wintner [2], Theorem 5). In fact, $g(e)$ in (4) is merely assumed to be of class L^2 on Σ. But if $g(e)$ is not bounded (almost everywhere) on Σ, then (4) and (7) imply that the spectrum of $\phi_n(E)$ is not a bounded set for sufficiently large n].

It will be assumed that (8) is convergent, i. e., that (9) defines a distribution function $\phi = \phi(E)$. The Fourier-Stieltjes transform of this ϕ is

(10) $$\Lambda(u;\phi) = \prod_{n=1}^{\infty}\Lambda(u;\phi_n).$$

Comparison of (6) with (5) also shows that the infinite product (10) is absolutely convergent for every u, the series (8) being convergent. Furthermore, from (2) and (1),

$$|\Lambda(u;\phi_n)| \leqq \int d\Sigma_e = 1.$$

Hence, the absolute value of the infinite product (10) is not increased if one omits some of its factors; so that

$$(11) \qquad |\Lambda(u;\phi)| \leqq \prod_{\rho_n < N(u)} |\Lambda(u;\phi_n)|$$

holds for every u and for an arbitrary function N of u.

Since the constant α occurring in the first of the inequalities (6) is positive, the asymptotic formula (5), when applied to $\rho = \rho_n$, is seen to imply the existence of a positive constant γ which has the property that

$$(12) \qquad |\Lambda(u;\phi_n)| \leqq \exp\{-\tfrac{1}{3}\alpha\rho_n{}^2u^2\} \text{ whenever } \rho_n\,|u| < \gamma.$$

On placing $N(u) = \gamma/|u|$ for an arbitrary $u \neq 0$, the estimates (11) and (12) are seen to imply that the inequality

$$|\Lambda(u;\phi)| \leqq \exp\{-\tfrac{1}{3}\alpha u^2 \sum_{\rho_n < \gamma/|u|} \rho_n{}^2\} \qquad (\gamma = \text{const.} > 0)$$

holds for every $u \neq 0$. Consequently, *there exist two positive constants* γ, c $(=\frac{1}{3}\alpha)$ *such that*

$$(13) \qquad \Lambda(u;\phi) = O(\exp\{-cu^2K(\gamma/|u|)\}) \text{ as } |u| \to \infty,$$

where

$$(14) \qquad K(v) = \sum_{\rho_n < v} \rho_n{}^2 \qquad (v > 0).$$

In order to apply the estimate (13)–(14) of (10) to the questions mentioned in the introduction, suppose first that the given sequence $\rho_1, \rho_2, \cdots$ of positive numbers is of the type

$$(15) \qquad \rho_n \sim \text{const.}\, n^{-\sigma}, \qquad n \to \infty, \qquad (\text{const.} > 0),$$

where σ is a constant; since (8) is supposed to be convergent, $\sigma > \frac{1}{2}$. From (15) and (14),

$$K(v) \sim \text{Const.} \sum_{n^{-\sigma} < v} n^{-2\sigma} \sim \text{Const.} \int_{v^{-1/\sigma}}^{\infty} n^{-2\sigma} dn \text{ as } v \to \infty,$$

where Const. > 0; so that

$$K(v) \sim (1-2\sigma)^{-1} \text{ Const. } v^{2-1/\sigma} \text{ as } v \to \infty.$$

Hence, from (13),

$$(16)\qquad \Lambda(u;\phi)=O(\exp\{-C\,|\,u\,|^{1/\sigma}\})\ \text{ as }\ |\,u\,|\to\infty,$$

where $C=c(1-2\sigma)^{-1}\gamma^{2-1/\sigma}$ Const. is a positive constant.

Similarly, if (15) is replaced by the more general condition that, for some fixed σ $(>\frac{1}{2})$ and for any given $\delta>0$,

$$(17)\qquad \text{const.}\ n^{-\sigma-\delta}<\rho_n<\text{const.}\ n^{-\sigma+\delta}\ \text{ as }\ n\to\infty,$$

where the positive const. may depend on δ, then, again from (13)–(14),

$$(18)\qquad \Lambda(u;\phi)=O(\exp\{-C\,|\,u\,|^{(1-\epsilon)/\sigma}\})\ \text{ as }\ |\,u\,|\to\infty,$$

where $C=C_\epsilon$ is positive and independent of u, while $\epsilon>0$ is arbitrary.

Condition (17) is satisfied for every $\delta>0$ if

$$(19)\qquad \rho_n=p_n^{-\sigma},$$

where p_n is the n-th prime number. This is clear from the elementary inequalities of Chebycheff, since these imply that the ratio $p_n:n\log n$ remains between two positive bounds as $n\to\infty$.

Now it is known that if the Fourier-Stieltjes transform $\Lambda(u;\psi)$ of a distribution function $\psi=\psi(E)$ is such that

$$\Lambda(u;\psi)=O(|\,u\,|^{-q}),\qquad |\,u\,|\to\infty$$

holds for every fixed $q>0$, then $\psi(E)$ is absolutely continuous with a density for which all derivatives exist and are uniformly continuous in the x-space. In particular, this will be the case if

$$(20)\qquad \Lambda(u;\psi)=O(\exp\{-C\,|\,u\,|^{\lambda}\}),\qquad |\,u\,|\to\infty,$$

holds for some pair of positive constants C, λ. If, in addition, one can choose $\lambda=1$ in (20), then the density is regular analytic and bounded in a "strip" about the real domain, with a "width" which tends with C to ∞; so that the density of ψ is a transcendental entire function if one can choose $\lambda>1$ in (20).

Since (18) means that $\psi=\phi$ satisfies (20) for every λ which is less than $1/\sigma$, it follows that, in the case (17), the infinite convolution (9) is absolutely continuous with a density for which all partial derivatives exist and are uniformly continuous in the x-space; and that this density is a transcendental entire function if $1>\sigma$ $(>\frac{1}{2})$.

As far as the conditions imposed on the mapping $x=f(\rho e)$ are concerned, notice that if the k components of the vector function f are regular harmonic

functions of j variables in a sphere about the origin of these j variables, and vanish in the first order at this origin in such a way as to have there a Jacobian matrix of rank k, then all the conditions (3), (4), (4 bis), (6) are obviously satisfied. If, in particular, $j = 2 = k$, one can choose the components of $f(\rho e)$ to be the real and imaginary parts of any power series

$$F(z) = c_1 z + c_2 z^2 + \cdots \text{ such that } c_1 \neq 0 \text{ and } \limsup |c_n|^{1/n} < \infty.$$

Now, in the asymptotic distribution theory of (the logarithm of) the Riemann zeta-function (cf. Jessen and Wintner [2]) one has simply

$$F(z) = -\log(1 - z) = z + \tfrac{1}{2}z^2 + \tfrac{1}{3}z^3 + \cdots,$$

while the ρ_n are given by the particular case (19) of (17).

It may be mentioned that the above elementary method also applies in problems of the type occurring in connection with the logarithmic derivative of the Riemann zeta-function (cf. Kershner and Wintner [3]).

THE JOHNS HOPKINS UNIVERSITY.

REFERENCES.

[1] E. K Haviland and A. Wintner, "On the Fourier transforms of distributions on convex curves," *Duke Mathematical Journal*, vol. 2 (1936), pp. 712-721.

[2] B. Jessen and A. Wintner, "Distribution functions and the Riemann zeta function," *Transactions of the American Mathematical Society*, vol. 38 (1935), pp. 48-88.

[3] R. Kershner and A. Wintner, "On the asymptotic distribution of in the critical strip," *American Journal of Mathematics*, vol. 59 (1937), pp. 673-678.

[4] A. Wintner, "Upon a statistical method in the theory of diophantine approximations," *American Journal of Mathematics*, vol. 55 (1933), pp. 309-331.

[5] A. Wintner, "On symmetric Bernoulli convolutions," *Bulletin of the American Mathematical Society*, vol. 41 (1935), pp. 137-138.

THE FOURIER SERIES AND THE FUNCTIONAL EQUATION OF THE ABSOLUTE MODULAR INVARIANT $J(\tau)$.*

By Hans Rademacher.

1. The Fourier expansion for the absolute modular invariant $J(\tau)$ is

$$(1.1)\qquad 12^3 J(\tau) = e^{-2\pi i\tau} + 744 + \sum_{n=1}^{\infty} c_n e^{2\pi i n\tau}$$

with

$$(1.2)\qquad c_n = \frac{2\pi}{\sqrt{n}} \sum_{k=1}^{\infty} \frac{A_k(n)}{k} I_1\left(\frac{4\pi\sqrt{n}}{k}\right),$$

$$(1.3)\qquad A_k(n) = \sum_{\substack{h \bmod k \\ (h,k)=1}} \exp\left[-\frac{2\pi i}{k}(nh+h')\right], \qquad hh' \equiv -1 \pmod{k}.$$

This expansion was first given by H. Petersson in 1932.[1] I regret not having been aware of Petersson's priority when I recently published it again.[2] Our two proofs, however, have nothing in common, since they approach the problem from two opposite sides. Petersson discusses modular forms of *negative* dimension $r \leqq -2$. The derivative $J'(\tau)$ is clearly of dimension -2. By means of his generalized Poincaré series Petersson constructs a modular form of dimension -2, of which he shows, through a theorem of uniqueness, whose application in this case he briefly indicates, that it must be identical with $J'(\tau)$. By expanding his Poincaré series into a Fourier series he finds the series for $J'(\tau)$ and by integration that for $J(\tau)$. On the other hand, my method is a refinement of my variant of the Hardy-Ramanujan method, which originally was only applicable to modular forms of *positive* dimension. The Kloosterman method permitted its extension to modular forms of dimension zero.[3]

---

* Received August 26, 1938.

[1] Hans Petersson, "Ueber die Entwicklungskoeffizienten der automorphen Formen," *Acta Mathematica*, Bd. 58, pp. 169-215, in particular p. 202.

[2] "The Fourier coefficients of the modular invariant $J(\tau)$," *American Journal of Mathematics*, vol. 60 (1938), pp. 501-512. I avail myself of this opportunity to supplement a remark in that paper. When I mentioned there (p. 511) that only the numerical values of c_1 and c_2 seemed to appear in the literature I had overlooked the paper of W. E. H. Berwick, "An invariant modular equation of the fifth order," *Quarterly Journal of Mathematics*, vol. 47 (1916), pp. 94-103, in which the author gives the numerical values of the coefficients up to c_7.

[3] The present paper had, with another introduction, already been submitted for

If we leave aside a normalizing constant factor and an additive constant the modular function $J(\tau)$ is unambiguously characterized as the function regular in the upper τ-half-plane, having a pole of the first order at $x=0$ for the variable $x=e^{2\pi i\tau}$ and satisfying the functional relations

$$J(\tau)=J(\tau+1), \tag{1.4}$$

$$J(\tau)=J(-1/\tau). \tag{1.5}$$

The problem we are dealing with in this paper is so to speak the converse of that of determining the series (1.1) for the modular function $J(\tau)$. We ask here: given the expansion (1.1), how can we see that it represents a modular function, i.e. that the function defined by the expansion satisfies the above mentioned functional relations? Now it is obvious that (1.1) as a Fourier series has the property (1.4). We are therefore only concerned with (1.5).

Our method will, in brief words, consist in a transformation carrying (1.1) over into a certain double series. In this double series, which is not absolutely convergent, we shall have to interchange the summations with respect to the two indices of summation. The greatest part of our conclusion will be purely formal. Since only the treatment of the double series involves some analytical intricacies, we shall deal with it in a separate lemma, which we prove first, in order not to interrupt the continuity of the main reasonings.

2. Lemma. *Let τ be complex with positive imaginary part. Then*

$$\sum_{k=1}^{\infty}\lim_{N\to\infty}\sum_{\substack{m=-N\\(m,k)=1}}^{+N}\frac{e^{-(2\pi i m'/k)}}{k(k\tau-m)}=\lim_{K\to\infty}\sum_{k=1}^{K}\sum_{\substack{m=-K\\(m,k)=1}}^{+K}\frac{e^{-(2\pi i m'/k)}}{k(k\tau-m)}, \tag{2.1}$$

where m' is defined as a solution of the congruence

$$mm'\equiv -1 \pmod{k}.$$[4]

Proof. We first prove the convergence of the left-hand side of (2.1). We have

$$\sum_{\substack{m=-N\\(m,k)=1}}^{+N}\frac{e^{-(2\pi i m'/k)}}{k(k\tau-m)}=\frac{1}{k}\sum_{\substack{h \bmod k\\(h,k)=1}}e^{-(2\pi i h'/k)}\sum_{\substack{n\\|nk+h|\leq N}}\frac{1}{k\tau-h-nk};$$

hence

publication, when on September 14th, 1938, I received a letter from Professor Petersson, drawing my attention to his previous publication.

[4] The dash $'$ is used in this meaning throughout this paper; the modulus of the defining congruence will always be clearly stated by the context.

$$\lim_{N\to\infty} \sum_{\substack{m=-N \\ (m,k)=1}}^{+N} \frac{e^{-(2\pi i m'/k)}}{k(k\tau - m)} = \frac{1}{k^2} \sum_{\substack{h \bmod k \\ (h,k)=1}} e^{-(2\pi i h'/k)} \lim_{N\to\infty} \sum_{\substack{n \\ |nk+h| \leq N}} \frac{1}{\tau - h/k - n}$$

$$= \frac{1}{k^2} \sum_{\substack{h \bmod k \\ (h,k)=1}} e^{-(2\pi i h'/k)} \cdot 2\pi i \left(\tfrac{1}{2} - \frac{1}{1 - e^{2\pi i(\tau - h/k)}}\right)$$

$$= \frac{\pi i}{k^2} \mu(k) - \frac{2\pi i}{k^2} \sum_{\substack{h \bmod k \\ (h,k)=1}} e^{-(2\pi i h'/k)} \sum_{\nu=0}^{\infty} e^{2\pi i \nu(\tau - h/k)},$$

$$(2.2) \quad \lim_{N\to\infty} \sum_{\substack{m=-N \\ (m,k)=1}}^{+N} \frac{e^{-(2\pi i m'/k)}}{k(k\tau - m)} = \frac{\pi i \mu(k)}{k^2} - \frac{2\pi i}{k^2} \sum_{\nu=0}^{\infty} e^{2\pi i \nu \tau} \sum_{\substack{h \bmod k \\ (h,k)=1}} \exp\left[-\frac{2\pi i}{k}(h' + h\nu)\right].$$

Now the inner sum of the last term is a Kloosterman sum, for which we have, after Estermann, Salié and Davenport,[5] the estimate

$$(2.31) \quad \sum_{\substack{h \bmod k \\ (h,k)=1}} \exp\left[-\frac{2\pi i}{k}(h' + h\nu)\right] = O(k^{2/3+\epsilon}).$$

We put

$$(2.32) \quad \tau = \alpha + \beta i, \qquad \beta > 0$$

and obtain

$$\sum_{\nu=0}^{\infty} e^{2\pi i \nu \tau} \sum_{\substack{h \bmod k \\ (h,k)=1}} \exp\left[-\frac{2\pi i}{k}(h' + h\nu)\right] = O\left(k^{2/3+\epsilon} \frac{1}{1 - e^{-2\pi\beta}}\right).$$

Consequently from (2.2)

$$(2.33) \quad \lim_{N\to\infty} \sum_{\substack{m=-N \\ (m,k)=1}}^{+N} \frac{e^{-(2\pi i m'/k)}}{k(k\tau - m)} = O\left(k^{-(4/3)+\epsilon} \frac{1}{1 - e^{-2\pi\beta}}\right).$$

This shows the convergence of the first sum in (2.1).

We now can enunciate the lemma in the following form

$$(2.4) \quad \lim_{K\to\infty} \sum_{k=1}^{K} \lim_{N\to\infty} \sum_{\substack{K < |m| \leq N \\ (m,k)=1}} \frac{e^{-(2\pi i m'/k)}}{k(k\tau - m)} = 0,$$

in which form we are going to prove it.

We first consider

$$(2.5) \quad T_k^{(K)} = \lim_{N\to\infty} T_k^{(K,N)} = \lim_{N\to\infty} \sum_{\substack{K < |m| \leq N \\ (m,k)=1}} \frac{e^{-(2\pi i m'/k)}}{k(k\tau - m)}.$$

Now the function

$$(2.61) \quad g(m) = \begin{cases} e^{-(2\pi i m'/k)} & \text{for } (m,k) = 1, \\ 0 & \text{otherwise} \end{cases}$$

---

[5] For references cf. my paper cited in footnote 2.

is periodic modulo k and can therefore be expressed as a " finite Fourier sum "

$$g(m)=\sum_{j=1}^{k}B_{j,k}e^{2\pi ijm/k}. \tag{2.62}$$

The coefficients $B_{j,k}$ are found in the customary way:

$$\sum_{m=1}^{k}g(m)e^{-(2\pi ilm/k)}=\sum_{j=1}^{k}B_{j,k}\sum_{m=1}^{k}e^{2\pi i(j-l)m/k}=kB_{l,k},$$

$$B_{j,k}=\frac{1}{k}\sum_{m=1}^{k}g(m)e^{-(2\pi ijm/k)},$$

$$B_{j,k}=\frac{1}{k}\sum_{\substack{m=1\\(m,k)=1}}^{k}\exp\left[-\frac{2\pi i}{k}(m'+jm)\right]. \tag{2.63}$$

Here we have again a Kloosterman sum, so that

$$B_{j,k}=O(k^{-1/3+\epsilon}). \tag{2.64}$$

We note separately the special case $j=k$:

$$B_{j,k}=\frac{1}{k}\sum_{\substack{m=1\\(m,k)=1}}^{k}e^{-(2\pi im'/k)}=\frac{\mu(k)}{k}. \tag{2.65}$$

The formulae (2.61), (2.62) and (2.65) permit us to transform $T_k^{(K,N)}$ of (2.5):

$$\begin{aligned}T_k^{(K,N)}&=\sum_{K<|m|\leq N}\sum_{j=1}^{k}B_{j,k}\frac{e^{2\pi ijm/k}}{k(k\tau-m)}\\&=\sum_{j=1}^{k-1}B_{j,k}\sum_{K<|m|\leq N}\frac{e^{2\pi ijm/k}}{k(k\tau-m)}+\frac{\mu(k)}{k}\sum_{K<|m|\leq N}\frac{1}{k(k\tau-m)}.\end{aligned}$$

This leads to

$$\begin{aligned}T_k^{(K)}&=\lim_{N\to\infty}T_k^{(K,N)}\\&=\frac{1}{k}\sum_{j=1}^{k-1}B_{j,k}\sum_{m=K+1}^{\infty}\frac{e^{2\pi ijm/k}}{k\tau-m}+\frac{1}{k}\sum_{j=1}^{k-1}B_{j,k}\sum_{m=K+1}^{\infty}\frac{e^{-(2\pi ijm/k)}}{k\tau+m}\\&\quad+\frac{\mu(k)}{k^2}\sum_{m=K+1}^{\infty}\left(\frac{1}{k\tau-m}+\frac{1}{k\tau+m}\right)=S_1+S_2+S_3,\end{aligned} \tag{2.7}$$

say. The convergence of the infinite sums will be shown incidentally.

With the notation (2.32) we have [6]

---

[6] The following estimations could be considerably shortened and simplified if we were to content ourselves with the special case of purely imaginary τ. In fact, this would suffice to prove the relation (1.5) under the same restriction, which then could be lifted by the principle of analytic continuation. However, I have not chosen this way since for the purpose of this paper it seems to me more natural to leave τ as unrestricted as is compatible with the sense of (1.1).

$$S_3=\frac{\mu(k)}{k^2}\left\{\sum_{m=K+1}^{\infty}\left(\frac{1}{(\alpha+i\beta)k-m}-\frac{1}{i\beta k-m}\right)\right.$$
$$+\sum_{m=K+1}^{\infty}\left(\frac{1}{(\alpha+i\beta)k+m}-\frac{1}{i\beta k+m}\right)$$
$$\left.+\sum_{m=K+1}^{\infty}\left(\frac{1}{i\beta k-m}+\frac{1}{i\beta k+m}\right)\right\},$$

$$|S_3|\leqq\frac{1}{k^2}\left\{\sum_{m=K+1}^{\infty}\frac{|\alpha|k}{((\alpha k-m)^2+\beta^2k^2)^{\frac12}(m^2+\beta^2k^2)^{\frac12}}\right. \tag{2.81}$$
$$\left.+\sum_{m=K+1}^{\infty}\frac{|\alpha|k}{((\alpha k+m)^2+\beta^2k^2)^{\frac12}(m^2+\beta^2k^2)^{\frac12}}+\sum_{m=K+1}^{\infty}\frac{2\beta k}{m^2+\beta^2k^2}\right\}$$
$$<\frac{1}{k}\left\{\sum_{m=K+1}^{\infty}\frac{2|\alpha|}{((|\alpha|k-m)^2+\beta^2k^2)^{\frac12}m}+\sum_{m=K+1}^{\infty}\frac{2\beta}{m^2}\right\}$$
$$=\frac{1}{k}(S_3'+S_3'').$$

Here we have

$$S_3''<\int_K^{\infty}\frac{2\beta dx}{x^2}=\frac{2\beta}{K}. \tag{2.82}$$

We write

$$S_3'=\sum_{K<m\leqq(|\alpha|+1)K}+\sum_{(|\alpha|+1)K<m}=s_1+s_2. \tag{2.83}$$

Now (2.4) shows that we always have

$$1\leqq k\leqq K.$$

Therefore we majorize the sum s_1 in (2.83) if we replace there the sequence

$$(|\alpha|k-m)^2,\qquad K<m\leqq(|\alpha|+1)K$$

by twice the sequence

$$m^2,\qquad 0\leqq m\leqq(|\alpha|+1)K;$$

so that

$$s_1\leqq4|\alpha|\sum_{0\leqq m\leqq(|\alpha|+1)K}\frac{1}{(m^2+\beta^2k^2)^{\frac12}K}$$
$$\leqq4|\alpha|\left(\frac{1}{\beta kK}+\sum_{1\leqq m\leqq(|\alpha|+1)K}\frac{1}{mK}\right)=O\left(\frac{\log K}{K}\right), \tag{2.84}$$

where we have suppressed under the O-symbol the irrelevant parameters α and β.

In s_2 we have

$$k\leqq K<\frac{m}{|\alpha|+1};$$

hence

$$m - |\alpha| k > m - \frac{|\alpha| m}{|\alpha| + 1} = \frac{m}{|\alpha| + 1}$$

Therefore

$$s_2 \leqq \sum_{(|\alpha|+1)K < m} \frac{2|\alpha|(|\alpha|+1)}{m^2} = O\left(\frac{1}{K}\right). \tag{2.85}$$

The inequalities (2.81), (2.82), (2.83), (2.84), (2.85) together show that

$$S_3 = O\left(\frac{\log K}{kK}\right), \qquad 1 \leqq k \leqq K. \tag{2.86}$$

For the estimation of S_1 we first consider a finite sum. We have

$$\sum_{m=K+1}^{N} \frac{e^{2\pi i j m/k}}{k\tau - m} = \left\{ \int_{N+\frac{1}{2}-\tau\infty}^{N+\frac{1}{2}+\tau\infty} - \int_{K+\frac{1}{2}-\tau\infty}^{K+\frac{1}{2}+\tau\infty} \right\} \frac{e^{2\pi i j z/k}}{k\tau - z} \frac{dz}{e^{2\pi i z} - 1}, \tag{2.91}$$

where the paths of integration are straight lines forming the angle

$$\delta = \arg \tau$$

with the positive real axis, where

$$0 < \delta < \pi. \tag{2.92}$$

The absolute convergence of the integrals is easily ascertained because of $1 \leqq j \leqq k - 1$. With

$$z = x + (\alpha + i\beta) t \tag{2.93}$$

we have

$$|e^{2\pi i j z/k}| = e^{-(2\pi j \beta t/k)}.$$

The denominator $(e^{2\pi i z} - 1)$ is different from zero on the paths of integration. For the question of convergence we can therefore disregard an interval around $t = 0$ and need only discuss $|t| \geqq 1$ in (2.93). We obtain

$$|e^{2\pi i z} - 1| \geqq |e^{-2\pi\beta t} - 1|;$$

hence

$$\left| \frac{e^{2\pi i j z/k}}{e^{2\pi i z} - 1} \right| \leqq \frac{e^{-(2\pi j \beta t/k)}}{|e^{-2\pi\beta t} - 1|}.$$

This shows the convergence of the integrals, as well as the uniform convergence of the integrand to zero with $|t| \to \infty$, for $K + \frac{1}{2} \leqq x \leqq N + \frac{1}{2}$. If we put

$$|\tau| \int_{-\infty}^{+\infty} \frac{e^{-(2\pi j \beta t/k)}}{|e^{2\pi i(\alpha+i\beta)t} + 1|} dt = C,$$

we have in particular for the first integral in (2.91)

$$\left| \int_{N+\frac{1}{2}-\tau\infty}^{N+\frac{1}{2}+\tau\infty} \right| \leqq C \operatorname*{Max}_{z=N+\frac{1}{2}+\tau t} \frac{1}{|k\tau - z|}$$
$$= C \operatorname*{Max}_{-\infty<t<\infty} \frac{1}{|\tau(k-t) - N - \frac{1}{2}|} = \frac{C}{(N+\frac{1}{2})\sin\delta},$$

which tends to zero with N tending to infinity. Hence

$$\sum_{m=K+1}^{\infty} \frac{e^{2\pi i j m/k}}{k\tau - m} = -\int_{K+\frac{1}{2}-\tau\infty}^{K+\frac{1}{2}+\tau\infty} \frac{e^{2\pi i j z/k}}{k\tau - z} \frac{dz}{e^{2\pi i z} - 1},$$

and so

$$\left| \sum_{m=K+1}^{\infty} \frac{e^{2\pi i j m/k}}{k\tau - m} \right| \leqq C \operatorname*{Max}_{z=K+\frac{1}{2}+\tau t} \frac{1}{|k\tau - z|} = \frac{C}{(K+\frac{1}{2})\sin\delta}.$$

If we introduce this into the definition (2.7) of S_1 and make use of (2.64) we obtain

(2.94) $$S_1 = O(k^{-(1/3)+\epsilon}K^{-1}).$$

The analogous estimate holds true for S_2. Combining (2.7), (2.86), and (2.94) we get

$$T_k^{(K)} = O(k^{-(1/3)+\epsilon}K^{-1}\log K), \qquad 1 \leqq k \leqq K.$$

From this we deduce further

$$\sum_{k=1}^{K} T_k^{(K)} = O(K^{-1}\log K \sum_{k=1}^{K} k^{-(1/3)+\epsilon}) = O(K^{-(1/3)+\epsilon}\log K).$$

In virtue of the definition (2.5) of $T_k^{(K)}$ this implies the assertion (2.4) and therefore proves the lemma.

3. We now proceed as follows. Putting

$$x = e^{2\pi i\tau},$$

we have from (1.1)

(3.1) $$f(x) = 12^3 J(\tau) = x^{-1} + 744 + \sum_{n=1}^{\infty} c_n x^n.$$

The function $f(x)$ is regular for $|x| < 1$ with the exception of $x = 0$. The convergence of the power series in $|x| < 1$ follows immediately from the asymptotic formula

$$c_n \sim \frac{1}{\sqrt{2}\, n^{3/4}} e^{4\pi\sqrt{n}},$$

which in turn is a corollary of (1.2).[7] The function $J(\tau)$, which in the present discussion we have to consider as *defined* by (1.1), is therefore analytic in the upper τ-half-plane.

Introducing (1.2) and (1.3) into (3.1) we obtain

$$\begin{aligned} f(x) &= x^{-1} + 744 + \sum_{n=1}^{\infty} x^n \frac{2\pi}{\sqrt{n}} \sum_{k=1}^{\infty} \frac{A_k(n)}{k} I_1\left(\frac{4\pi\sqrt{n}}{k}\right) \\ &= x^{-1} + 744 + 2\pi \sum_{k=1}^{\infty} \frac{1}{k} \sum_{n=1}^{\infty} A_k(n) \frac{x^n}{\sqrt{n}} I_1\left(\frac{4\pi\sqrt{n}}{k}\right) \\ &= x^{-1} + 744 + 2\pi \sum_{k=1}^{\infty} \frac{1}{k} \sum_{\substack{h \bmod k \\ (h,k)=1}} e^{-(2\pi i h'/k)} \sum_{n=1}^{\infty} (x e^{-(2\pi i h/k)})^n \frac{1}{\sqrt{n}} I_1\left(\frac{4\pi\sqrt{n}}{k}\right), \end{aligned}$$

$$12^3 J(\tau) = f(x) = x^{-1} + 744 + 2\pi \sum_{k=1}^{\infty} \frac{1}{k} \sum_{\substack{h \bmod k \\ (h,k)=1}} e^{-(2\pi i h'/k)} \Phi_k(x e^{-(2\pi i h/k)}) \tag{3.2}$$

with the notation

$$\Phi_k(z) = \sum_{n=1}^{\infty} \frac{1}{\sqrt{n}} I_1\left(\frac{4\pi\sqrt{n}}{k}\right) z^n = \sum_{n=1}^{\infty} g_k(n) z^n. \tag{3.3}$$

Here

$$g_k(w) = \frac{1}{\sqrt{w}} I_1\left(\frac{4\pi\sqrt{w}}{k}\right) = \frac{2\pi}{k} \sum_{\nu=0}^{\infty} \frac{\left(\frac{4\pi^2 w}{k^2}\right)^{\nu}}{\nu!\,(\nu+1)!} \tag{3.4}$$

is a transcendental entire function of order $\frac{1}{2}$. We remark that by a theorem of Wigert, the function $\Phi_k(z)$, which (3.3) defines only in the interior of the unit circle, can be continued analytically over the whole z-plane, with the exception of the point $z = 1$, where it has an essential singularity. The expansion (3.2) therefore shows a decomposition into "partial fractions" similar to that one which I have obtained in connection with the generating function of $p(n)$.[8] We do not pursue this remark here any further.

From (3.3) and (3.4) we infer

$$\begin{aligned} \Phi_k(z) &= \frac{2\pi}{k} \sum_{n=1}^{\infty} z^n \sum_{\nu=0}^{\infty} \frac{\left(\frac{4\pi^2}{k^2} n\right)^{\nu}}{\nu!\,(\nu+1)!} \\ &= \frac{2\pi}{k} \sum_{\nu=0}^{\infty} \frac{\left(\frac{2\pi}{k}\right)^{2\nu}}{\nu!\,(\nu+1)!} \sum_{n=1}^{\infty} n^{\nu} z^n. \end{aligned} \tag{3.5}$$

---

[7] Cf. Watson, *Bessel Functions*, p. 203, formula (2).

[8] "A convergent series for the partition function $p(n)$," *Proceedings of the National Academy of Sciences*, vol. 23 (1937), pp. 78-84.

For the transformation of the inner sum we make use of Lipschitz's formula [9]

$$\sum_{n=1}^{\infty} n^{\nu} e^{-2\pi t n} = \frac{\Gamma(\nu+1)}{(2\pi)^{\nu+1}} \sum_{l=-\infty}^{+\infty} \frac{1}{(t+li)^{\nu+1}},$$

which holds for $\Re(t) > 0$, $\nu > 0$. We can apply it on (3.5) if we put

$$z = e^{-2\pi t}. \tag{3.51}$$

For $\nu = 0$ we have

$$\sum_{n=1}^{\infty} e^{-2\pi t n} = -1 + \frac{1}{1-e^{-2\pi t}} = -\tfrac{1}{2} + \frac{1}{2\pi} \lim_{N\to\infty} \sum_{l=-N}^{+N} \frac{1}{t+li}$$

and so

$$\Phi_k(z) = \frac{2\pi}{k}\left\{ -\tfrac{1}{2} + \sum_{\nu=0}^{\infty} \frac{(2\pi/k)^{2\nu}}{\nu!\,(\nu+1)!}\; \frac{\nu!}{(2\pi)^{\nu+1}} \lim_{N\to\infty} \sum_{l=-N}^{+N} \frac{1}{(t+li)^{\nu+1}} \right\} \tag{3.61}$$

$$= -\frac{\pi}{k} + \lim_{N\to\infty} \frac{1}{k} \sum_{l=-N}^{+N} \sum_{\nu=0}^{\infty} \frac{1}{t+li} \frac{\left(\dfrac{2\pi}{k^2(t+li)}\right)^{\nu}}{(\nu+1)!}$$

$$= -\frac{\pi}{k} + \lim_{N\to\infty} \frac{1}{k} \sum_{l=-N}^{+N} \frac{1}{t+li} \cdot \frac{e^{2\pi/(k^2(t+li))} - 1}{2\pi/(k^2(t+li))},$$

$$\Phi_k(z) = -\frac{\pi}{k} + \lim_{N\to\infty} \frac{k}{2\pi} \sum_{l=-N}^{+N} \left(e^{2\pi/(k^2(t+li))} - 1\right). \tag{3.62}$$

We need in (3.2)

$$z = xe^{-(2\pi i h/k)} = e^{2\pi i(\tau - h/k)},$$

and therefore, because of (3.51),

$$t = -i\tau + i\,h\,.$$

Inserting this in (3.62), we obtain

$$\Phi_k(xe^{-(2\pi i h/k)}) = -\frac{\pi}{k} + \lim_{N\to\infty} \frac{k}{2\pi} \sum_{l=-N}^{+N} \left(e^{2\pi/ik(-k\tau+h+kl)} - 1\right) \tag{3.63}$$

$$= -\frac{\pi}{k} + \lim_{N\to\infty} \frac{k}{2\pi} \sum_{\substack{m\equiv h \pmod{k} \\ |m-h|\leqq kN}} \left(e^{2\pi i/k(k\tau-m)} - 1\right).$$

If we go back to the power series for the exponential function, viz. to (3.61), we see that for $\nu \geqq 1$ the limit process $N \to \infty$ may be carried out under the sign of summation with respect to l. For $\nu = 0$ the limit process

$$N \to \infty, \qquad |m-h| \leqq kN$$

is equivalent to

$$M \to \infty, \qquad |m| \leqq M,$$

---

[9] R. Lipschitz, "Untersuchung der Eigenschaften einer Gattung von unendlichen Reihen," *Journal für Mathematik*, Bd. 105 (1889), pp. 127-156, in particular p. 136.

since the single term

$$2\pi i/k(k\tau - m)$$

tends to zero as $|m| \to \infty$. The equation (3. 63) can therefore finally be written

$$(3.64) \quad \Phi_k(xe^{-(2\pi ih/k)}) = -\frac{\pi}{k} + \lim_{M\to\infty} \frac{k}{2\pi} \sum_{\substack{m\equiv h \pmod k \\ |m|\leq M}} (e^{2\pi i/k(k\tau-m)} - 1).$$

From this we obtain

$$\sum_{\substack{h \bmod k \\ (h,k)=1}} e^{-(2\pi ih'/k)}\Phi_k(xe^{-(2\pi ih/k)})$$

$$= -\frac{\pi}{k}\mu(k) + \lim_{M\to\infty} \frac{k}{2\pi} \sum_{\substack{|m|\leq M \\ (m,k)=1}} e^{-(2\pi im'/k)}(e^{2\pi i/k(k\tau-m)} - 1).$$

Returning to (3. 2) we get now

$$(3.7) \quad 12^3 J(\tau) = e^{-2\pi i\tau} + 744 - 2\pi^2 \sum_{k=1}^{\infty} \frac{\mu(k)}{k^2}$$

$$+ \sum_{k=1}^{\infty} \lim_{M\to\infty} \sum_{\substack{|m|\leq M \\ (m,k)=1}} e^{-(2\pi im'/k)}(e^{2\pi i/k(k\tau-m)} - 1).$$

The condition $(m, k) = 1$ implies that the value $m = 0$ can be assumed only together with $k = 1$. We separate this term. Furthermore we have

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

In consequence of these remarks, (3. 7) goes over into

$$(3.8) \quad 12^3 J(\tau) = e^{-2\pi i\tau} + e^{2\pi i/\tau} + 731$$

$$+ \sum_{k=1}^{\infty} \lim_{M\to\infty} \sum_{\substack{1\leq|m|\leq M \\ (m,k)=1}} \left(\exp\left(2\pi i \frac{\frac{mm'+1}{k} - m'\tau}{k\tau - m} \right) - \exp\left(-2\pi i \frac{m'}{k} \right) \right).$$

It is from this formula that we intend to derive the functional equation (1. 5).

4. For this purpose we have to show that (3. 8) can be replaced by

$$(4.1) \quad 12^3 J(\tau) = e^{-2\pi i\tau} + e^{2\pi i/\tau} + 731$$

$$+ \lim_{K\to\infty} \sum_{k=1}^{K} \sum_{\substack{1\leq|m|\leq K \\ (m,k)=1}} \left(\exp\left(2\pi i \frac{\frac{mm'+1}{k} - m'\tau}{k\tau - m} \right) - \exp\left(-2\pi i \frac{m'}{k} \right) \right).$$

It is, however, simpler to consider the infinite sum in the form which it has in (3. 7) instead of (3. 8). Indeed we have

$$S = \sum_{k=1}^{\infty} \lim_{M\to\infty} \sum_{\substack{|m|\leqq M \\ (m,k)=1}} e^{-(2\pi i m'/k)} \left(e^{2\pi i/k(k\tau-m)} - 1\right)$$

$$= \sum_{k=1}^{\infty} \lim_{M\to\infty} \sum_{\substack{|m|\leqq M \\ (m,k)=1}} e^{-(2\pi i m'/k)} \sum_{\lambda=1}^{\infty} \frac{1}{\lambda!}\left(\frac{2\pi i}{k(k\tau-m)}\right)^{\lambda},$$

$$S = \sum_{k=1}^{\infty} \lim_{M\to\infty} \sum_{\substack{|m|\leqq M \\ (m,k)=1}} e^{-(2\pi i m'/k)} \cdot \frac{2\pi i}{k(k\tau-m)} + \sum_{k=1}^{\infty} \sum_{\substack{m=-\infty \\ (m,k)=1}}^{+\infty} e^{-(2\pi i m'/k)} \sum_{\lambda=2}^{\infty} \frac{1}{\lambda!}\left(\frac{2\pi i}{k(k\tau-m)}\right)^{\lambda}. \tag{4.2}$$

The separation into two sums is permissible since both are convergent. This is true for the first in virtue of our lemma. The second sum is absolutely convergent in all three summations together and admits therefore any rearrangement of its terms. If we apply moreover our lemma to the first member on the right-hand side of (4. 2) we get

$$S = \lim_{K\to\infty} \sum_{k=1}^{K} \sum_{\substack{|m|\leqq K \\ (m,k)=1}} e^{-(2\pi i m'/k)} \cdot \frac{2\pi i}{k(k\tau-m)}$$

$$+ \lim_{K\to\infty} \sum_{k=1}^{K} \sum_{\substack{|m|\leqq K \\ (m,k)=1}} e^{-(2\pi i m'/k)} \sum_{\lambda=2}^{\infty} \frac{1}{\lambda!}\left(\frac{2\pi i}{k(k\tau-m)}\right)^{\lambda}$$

$$= \lim_{K\to\infty} \sum_{k=1}^{K} \sum_{\substack{|m|\leqq K \\ (m,k)=1}} e^{-(2\pi i m'/k)} \sum_{\lambda=1}^{\infty} \frac{1}{\lambda!}\left(\frac{2\pi i}{k(k\tau-m)}\right)^{\lambda}$$

$$= \lim_{K\to\infty} \sum_{k=1}^{K} \sum_{\substack{|m|\leqq K \\ (m,k)=1}} e^{-(2\pi i m'/k)} \left(e^{2\pi i/k(k\tau-m)} - 1\right).$$

This proves (4. 1).

5. The rest of our reasoning is now purely formal. The sum of the first three terms of the right-hand side of (4. 1) is invariant with respect to the transformation $\tau \to -1/\tau$. In order to establish (1. 5) we have therefore only to prove

$$\sum_{\substack{1\leqq k\leqq K \\ (m,k)=1}} \sum_{1\leqq|m|\leqq K} \left(\exp\left(2\pi i \frac{\dfrac{mm'+1}{k} - m'\tau}{k\tau - m}\right) - \exp\left(-2\pi i \frac{m'}{k}\right)\right)$$

$$= \sum_{\substack{1\leqq k\leqq K \\ (m,k)=1}} \sum_{1\leqq|m|\leqq K} \left(\exp\left(2\pi i \frac{\dfrac{mm'+1}{k}\tau + m'}{-k - m\tau}\right) - \exp\left(-2\pi i \frac{m'}{k}\right)\right).$$

Since these are finite sums we can suppress on both sides the identical second terms in the parentheses. Our assertion is therefore reduced to

$$
(5.1)\quad
\begin{aligned}
&\sum_{\substack{k=1\\(m,k)=1}}^{K}\sum_{m=1}^{K}\exp\left(2\pi i\frac{-k'-m'\tau}{k\tau-m}\right)+\sum_{\substack{k=1\\(m,k)=1}}^{K}\sum_{m=1}^{K}\exp\left(2\pi i\frac{-k'+m'\tau}{k\tau+m}\right)\\
=&\sum_{\substack{k=1\\(m,k)=1}}^{K}\sum_{m=1}^{K}\exp\left(2\pi i\frac{-k'\tau+m'}{-k-m\tau}\right)+\sum_{\substack{k=1\\(m,k)=1}}^{K}\sum_{m=1}^{K}\exp\left(2\pi i\frac{-k'\tau-m'}{-k+m\tau}\right).
\end{aligned}
$$

In this formula we have set

$$
(5.2)\qquad -k'=\frac{mm'+1}{k}.
$$

We have also used the fact that if m' belongs to m in

$$
(5.22)\qquad mm'\equiv -1 \pmod{k}
$$

then $-m'$ belongs to $-m$. The equation (5.2) is symmetric with respect to m and k, since

$$
(5.23)\qquad mm'+kk'+1=0;
$$

so that, corresponding to (5.22), we also have

$$
(5.24)\qquad kk'\equiv -1 \pmod{m}.
$$

We may write (5.1) in the more symmetrical form

$$
(5.3)\quad
\begin{aligned}
&\sum_{\substack{k=1\\(m,k)=1}}^{K}\sum_{m=1}^{K}\exp\left(-2\pi i\frac{m'\tau+k'}{k\tau-m}\right)+\sum_{\substack{k=1\\(m,k)=1}}^{K}\sum_{m=1}^{K}\exp\left(2\pi i\frac{m'\tau-k'}{k\tau+m}\right)\\
=&\sum_{\substack{k=1\\(m,k)=1}}^{K}\sum_{m=1}^{K}\exp\left(-2\pi i\frac{k'\tau+m'}{m\tau-k}\right)+\sum_{\substack{k=1\\(m,k)=1}}^{K}\sum_{m=1}^{K}\exp\left(2\pi i\frac{k'\tau-m'}{m\tau+k}\right).
\end{aligned}
$$

But this equation is obviously true, since one side goes over into the other by a mere change of notation, namely by replacing m, m' by k, k' and conversely.

We have therefore proved the functional property (1.5) as a consequence of the Fourier expansion (1.1) with the coefficients (1.2), (1.3).

UNIVERSITY OF PENNSYLVANIA,
PHILADELPHIA, PA.